ⵜⴰⵍⵖⵓⵙⵜ ⵜⴰⵏⴰⵎⵓⵔⵜ
الأمـن السـيبـراني

ترجمة ⴰⵙⵎⵍⵉ
ⵙⵍⵉⵎⴰ ⵍⴽⵓⵍⴰⵍⵉ
سليمة الكولالي

2024

+olJHO8+ +oΘΣΘΣΟIΣ+ +3IO3ΘΣOo+ +8OHIo+

ᑕᐅᓯᖅᑐᑦ ᑕᐅᑐᕐᔪᐊᑐᑦ

ᐅᑐᕐᓗᖅ

ᑐᓂᔭᕐᓂᐅ ᐃᕐᕿᓂᓂᔭ

2024

ⴰⵙⴳⵎⵓⵔ ⴰⵅⵏⴰⵍ ⵏ ⵜⵣⵙⵙⵏ ⵜⴰⵎⴰⵣⵉⵖⵜ
المعهد الملكي للثقافة الأمازيغية

ⴰⵎⵎⴰⵙ ⵏ ⵣⵙⵣⵢⵏ ⴷ ⵣⵏⵜⴰⵎ ⴷ ⵜⵣⵇⵉⵅⵜ ⴷ ⵣⵎⵔⴰⵍⴰⵉ
مركز الترجمة والتوثيق والنشر والتواصل

ⴰⵙⵏⴰⵢ : **العدد** 69 / ⵜⵉⵙⵙⵏ, ⵜⵉⵎⵓⵔⵜ ⵏ ⵜⵣⵙⵣⵢⵏ : **سلسلة** / ⴰⵙⵏⴰⵢ

العنوان / ⴰⵣⵍⵍⴰⵏ : **الأمن السيبراني** / ⵜⴰⵏⵍⵎⵙⵜ ⵜⴰⵙⵉⵖⵙⵉⵏⵉⵜ

المؤلف / ⴰⵎⵓⵔⵔ : **إدارة الدفاع الوطني – المديرية العامة لأمن نظم المعلومات**
ⵜⴰⵎⵓⵙⵙⵓⵜ ⵏ ⵣⵎⵣⴰⵢ ⴰⵏⵎⵙⵙ –
ⵜⴰⵎⵎⴰⵏ ⵜⴰⵎⴰⵜⴰⵔⵜ ⵉ ⵜⵍⵍⵙⵜ ⵏ ⵉⵍⵓⵙⴰⵍⵍ ⵏ ⵍⵜⵎⴰⵏ

المترجمة / ⵜⴰⵎⵓⵙⵙⵏⵜ : **سليمة الكولالي** / ⵙⴰⵍⵉⵎⴰ ⵍⴽⵓⵍⴰⵍⵉ

الإعداد والغلاف / ⴰⵙⵙⵏⵜⵜⴰⵏ ⵏ ⵜⵙⵙⵜⵜⴰⵏ : **نادية قيدي** / ⵏⴰⵔⵔⴰ ⵇⵉⴷⵉ

التتبع التقني / ⵜⵉⵜⵇⵍⵉⵜ ⵜⴰⵜⵉⵇⵓⵉⵜ : ⴰⵎⵎⴰⵙ ⵏ ⵣⵙⵣⵢⵏ ⴷ ⵣⵏⵜⴰⵎ ⴷ ⵣⵎⵔⴰⵍⴰⵉ
مركز الترجمة والتوثيق والنشر والتواصل

الطبع / ⴰⵙⵜⵜⵓⵔ : **مطبعة منشورات عكاظ** / ⵜⴰⵙⵜⵜⵓⵔⵜ ⵏ ⵜⵣⵇⵉⵅⵜ ⵏ ⵃⵙⵇⴰⵉ

الإيداع القانوني / ⴰⵙⵙⵙⵙ ⵙⵏⵅⵜ : 2024MO4813

ردمك / ⵙⵜⵉⵙⵏ ⴰⵅⵙⴰⵢⵏⴰⵏ ⴰⵏⴰⵎⴰⵔ ⵏ ⵙⴷⵏⵉⵙⵙ : 978-9920-520-22-5

حقوق الطبع / ⵜⵣⵙⵙⵓⵔ : © **المعهد الملكي للثقافة الأمازيغية**
ⴰⵙⵙⵏⵓⵔ ⴰⵅⵏⴰⵍ ⵏ ⵜⵣⵙⵙⵏ ⵜⴰⵎⴰⵣⵉⵖⵜ

ⵜⵣⵙⵙⵓⵔⴰⵍ ⵏ ⵙⵎⵅⵓⵔⵔ ⵜⵜⵍⴰⵎⵓⵔⵔⵍ. ⵜⵅⵏⵏ ⵍⴰⵏⴰⵙ ⵏ ⵜⵣⵇⵉⵅⵜ ⵉⵉⵅ ⴰⵙⵙⵏⵜ ⵏ ⵙⵏⵏⵉⵙⵙ ⵉⵉⵅ ⵛⴰ ⵏ ⵙⵅⵣⵣⵙⵎ ⵣⵣⴰⵙⵙⵓⵔ ⵉⵉⵅ ⴰⵅⵎⵎⵙ
ⵍⵍⵙ ⵅ ⵜⵎⴰⵙⵙⵙⵏ ⵉⵉⵅ ⵜⴰⵍⴰⵙⵙⵎⵜ ⵜⴰⵏⵜⵜⵇⵜⵙⵉⵜ ⵉⵉⵅ ⴰⵎⵎⵜⵜⵙⵉⵜ ⵍⵍⵙ ⵙ ⵛⴰ ⵏ ⵍⴰⵎⵎⵍⴰⵏⵅ ⵍⵍⵙⵉⵍ ⵉⵉⵅ ⴰⵍⵍⵏⵅ ⵍⵍⵙ ⵉⵉⵅ
ⴰⵙⵙⵙⵙ ⵍⵍⵙ ⵙ ⵎⴰⵎⵛ ⵎⵎⴰ ⵣⵎⵣⵣ ⵏⴰⵜ ⵏ ⵜⵙⵙⴰⵅⵜ ⵣⵜⵜⵔⴰⵙⴰⵏ ⵏ ⵙⵎⵣⵣⵙⵙⵏ.

ᓂᕆᓂᐱᕐᑫ ᓂᐧᐣᓂᑕᕐᐦ ᕿᕆᕿᕐᓂ 1.20 .69 ᕕᐦᐦᓭᐯ ᐱ ᐱᕐ 4 ᐱᕐ ᐃᐱᕐᐦᐦᓂ 1441 (25 ᖃᕿᐃᖃᕿᙵ 2020) ᕐ ᕿᙵᙵᐧᕐᑕᑎ ᑦ ᕿᙵᑎᐦ ᕿᕆᕿᕐᓂ 05 .20 ᕐᑫᑫᑦᑦ ᑎ ᖁᓂᐲᑐᕆ ᖁᓂᑕᕆᑕᑎᓯᖁ.

———

ᖁᓂᒪᓂᖅ ᕐ ᑫᕆᕆᕐ,
ᕐᖁᐃᕐ ᓂᐧᑭᓂᑕᕐᐦ – ᐱᐧᕉ ᕿᕉᑎᑎᕿ ᑦᑎ :
(ᒪᕿᐱᒪᒪᐱ ᕆᑎ ᐃᐱᓂᑎᓂᑎ ᕆᑎ ᒪᕿᐱᒪᒪᐱ ᕆᑎ ᖃᕿᑎᑦᐦ ᓂᐱ ᖅᕐᐱᑎ ᖃᕐᐃᕐ ᑫᕆᕆᕐ)

ᕐᖁᖁᒪᓂᑎᑎᑦ ᙵቧᕉ ᕿᕐᓂᑕᕐᑫ ᓂ ᑦᑎᖅ ᓂᐧᑭᓂᑕᕐᐦ ᖃᓂᖁᖁᕿᕿᑦ, ᓂᙆᙆᓂ :
ᑎ ᒪᓂᒪᑭ ᕐ ᐱ ᖃᕿᑎᓂ ᐱᕉ ᕿᐱᕿᑎᖁᕿᑎᑐ, ᐃᕿᒪᒪᑦ ᕐᒪᑦᑦᕐᖁᑦ 42 ᐱ 50 ᙵᙵᓂᕉᑎᓂ,

ᑦᒪᑭᓂ ᓂᓂᕐ ᑦᑎᖅ ᓂᐧᑭᓂᑕᕐᐦ ᕉᐦ ᒪᓂᓂ ᓂ :

ᕐᖁᖁᒪᓂᙵᙵᕉᑎᑐ, ᕐᖁᖁᒪᓂᙵᑫᕉ ᐱᕉ ᕿᖅᒪᕐᕆᑎ ᓂᒪᓂᐱᐱᕿᐱ, ᐱᐦᐦᕐᑐ ᕐ ᕿᕐᓂᑕᕐᑫ ᓂ ᑦᑎᖅ ᓂᑭᓂᑕᕐᐦ, ᓂᙵᑎᐦ ᕿᕐᕐᒪᕿ 05.20 ᕐᙆᙆᑦᑦ ᑎ ᖁᑦᐦᑎᕿ ᖁᓂᓂᑕᑎᑎᕿᖁᕿ, ᑎ ᒪᓂᒪᑭ ᕐ ᐯᓂᐦᑎ ᕐᒪᑎᓂᓂ ᕿᑎᓂᓂᒪᒪᕐᑦ ᑦ ᕐᒪᓂᓂᓂ ᐱ ᕿᑎᙆᙆᕐᑦ ᑦ ᕐᒪᑭᑭᕐᒪᓂᑫ.

ᕐᖁᖁᒪᓂᑎᕐ ᐱᕐ ᖁᕐᕓᒪᓂ ᐱᕐ 4 ᐱᕐ ᐃᐱᕐᑦᑦᓂ 1441 (25 ᖃᕿᐃᖃᕿᙵ 2020).

ᕐᑎᑎᐧᒪᒪᕐᕓ ᐯᓂᐦᑎ ᑎ ᕿᙵᐱᐱᕿᖃ :

ᓂᑎᑎᕐᕆᐯᐦ ᑦ ᖁᑎᓂᕓᖁ,
ᓂᑎᐧᒪᒪᕓ : ᑎᓴᐱ ᐱᐱᕐᑦ ᐃᓴᕿᖁᒪᓂᕐ

ᓄᓇᑕᖅ ᐱᕕᐱᒍ 05.20 ᕿᑭᑎᒪ ᐅ ᖃᐃᑦᑐᖅ ᖃᓄᐊᕐᓂᑕᖅ

ᓄᑕᙵᑕᓂᐊᓕ ᓄᒥᔪᑎᑕᑐᖅ : ᕿᐅᖃᐱᓂᐱᒪ ᕿᑕᓂᖃᓕᒫ

ᓄᑕᑎᕿ 1

ᕿᐅᒪᖅᑦᑦᖅ ᖅᓇᑕᕐᓂ ᓄ :

- ᕿᐊᖅᙴᑎᒪ ᐱ ᕿᐅᒪᓄᑕᑎ ᐃ ᖃᐃᑦᑐᖅ ᖅᐅᐃᕿᐅᑎ ᙴᕐ ᕿᐃᙴᑕᓄᒪᒪᑎ ᐃ ᒪᖅᑕᐋᓂᒪ ᐃ ᖃᑕᐅᐅᙴᑕᑕᕿᑎ ᐃ ᒪᓄᑕᓂᐊ ᒪᓄᖅᓂᑎ ᐃ ᖃᑕᐅᐅᓂᓂᓕ ᖃᕿᙴᐱᖅᓂᒪᒪᑎ ᐃ ᑕᖅ ᖅᐱᑕ ᓄᒪᒪᙴᑕ ᒪᒪᕿᕿᑕ ᓄᑫᑫᓄ ᖃ ᓄᐱᖅ ᐃ ᖅᓇᑕᕐᓂ ᓄᑕᓂᖃᓂᓄᒪᒪ ᐱᙴ ᖅᓇᑕᕐᓂ ᓄ;

- ᕿᐊᖅᙴᑎᒪ ᐱ ᕿᐅᒪᓄᑕᑎ ᐃ ᖃᐃᑦᑐᖅ ᖅᐅᐃᕿᐅᑎ ᙴᕐ ᖃᖅᑐᕿᒪᑎᑕᑎ ᖃᕿᓂᐱᐱᓄᒪᑎᑕᑎ ᖃᕿᑕᓄᐱᑕᓄᒪᕿᑎ;

- ᕿᐊᖅᙴᑎᒪ ᐱ ᕿᐅᒪᓄᑕᑎ ᐃ ᖃᐃᑦᑐᖅ ᖅᐅᐃᕿᐅᑎ ᙴᕐ ᕿᑕᐅᓱᐊᐊᓂ ᐃ ᕿᐃᕮᒪᓄᒪ ᕿᑕᓂᖃᓂᓄᒪ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᖃᑕᐅᑕᐃᕿᐱᑎ ᐃ ᖃᐃᑦᑐᖅ ᖃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᖃᐃᑦᑐᖅ ᖃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᖃᐃᑦᑐᖅ ᖃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᖃᑕᖅᑫᓗ ᐃ ᕿᐱᐅᑎᓗᓕᑎ ᐃ ᒪᓄᐃᑦᑐᖅᑦ, ᐃᐃᕿᑎ ᓄᐅᐃ ᐱᙴ ᖅᓇᑕᕐᓂ ᓄ “ᓄᑕᙵᓄᕐᕿᓄᒪ”;

- ᓄᐅᓄᐃᕿ ᓄᓄᑕᖅᑐ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃ ᐃᑐᖅᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ;

- ᓄᐅᓄᐃᕿ ᐃ ᖅᑕᙵᓄᒪᓄᐅ ᐱ ᖅᑕᑕᐅᑎᓄ᙭ ᐃ ᒪᖅᑕ᙭ᒪ ᙆᐅ ᐃᐃᓄᕮᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᐃᐃᑐᖅᑦ ᓄᑕᑐᖅᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᖅᑫᑫᓄ᙭ ᐃ ᐃᐱᑎᑫᓕᓄᒪᑎ ᐃ ᒪᓄᐃᑦᑐᖅᑦ, ᐃᐃᕿᑎ ᓄᐅᐃ ᐱᙴ ᖅᓇᑕᕐᓂ ᓄ “ᓄᑕᙵᓄᕐᕿᓄᒪ”;

- ᓄᐅᓄᐃᕿ ᓄᓄᑕᖅᑐ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ;

- ᓄᐅᓄᐃᕿ ᐃ ᖅᑕᙵᓄᒪᓄᐅ ᐱ ᖅᑕᑕᐅᑎᓄ᙭ ᐃ ᒪᖅᑕ᙭ᒪ ᙆᐅ ᐃᐃᓄᕮᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᐃᐃᑐᖅᑦ ᓄᑕᑐᖅᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᖅᑫᑫᓄ᙭ ᐃ ᐃᐱᑎᑫᓕᓄᒪᑎ ᐃ ᒪᓄᐃᑦᑐᖅᑦ, ᐃᐃᕿᑎ ᓄᐅᐃ ᐱᙴ ᖅᓇᑕᕐᓂ ᓄ “ᓄᑕᙵᓄᕐᕿᓄᒪ”;

- ᓄᐅᓄᐃᕿ ᐃ ᖅᑕᙵᓄᒪᓄᐅ ᐱ ᖅᑕᑕᐅᑎᓄ᙭ ᐃ ᒪᖅᑕ᙭ᒪ ᙆᐅ ᐃᐃᓄᕮᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᐅᑕᐃᕿᐱᑎ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃ ᕿᑕᖅᑫᑫᓄ᙭ ᐃ ᐃᐱᑎᑫᓕᓄᒪᑎ ᐃ ᒪᓄᐃᑦᑐᖅᑦ, ᐃᐃᕿᑎ ᓄᐅᐃ ᐱᙴ ᖅᓇᑕᕐᓂ ᓄ “ᓄᑕᙵᓄᕐᕿᓄᒪ”;

- ᓄᐅᓄᐃᕿ ᓄᓄᑕᖅᑐ ᐃ ᐃᖅᖅᐅᕮᓄ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ ᐃᓄᐅᕿᐅᐃᕿᐃᑦ

ᑕᓂ ᐅᑕᏆᑫᓂ ᕿᕈᐃᖏ ᐅ ᖃᐅᓂᔪᑐᓂᑐ ᓂᐅᕿᐅᑐᓂᐊᕐᓂᒃ, ᕿᐦᑕᑐᓂ ᓂᐱ ᔪᓂᖅᓂ ᖁᖃᑦ ᐱ ᐅᐅᐊᓂᑕᖁ ᐱ ᖁᐃᖃᐊᓂ ᐅ ᖁᑕᖃᑕᓂ ᕿᖁᖁᓂᐊᑐᑐᑐᓂ ᐃᕈᖏ ᕿᖁᖁᓂᐊᓂᐅᑕᕐᐱᓂ ᐃᕈᖏ ᕿᖁᖁᓂᐊᓂᐊᕐᕿᕼᕈᐃ, ᐱ ᖁᖃᓂ ᕿᕈᐃᖏ ᕿ ᕿᐅᐅᑕᐃᕈᐱ ᖃᐃᐅᓂᐊᓗ ᓂ ᐃᕈᖏ ᕿᖁᖁᐃᐃᓂ ᓂᐱᓂᕼ ᖏᓂᐅᐅ ;

- **ᕿᐅᕐᕉᕿᕈᐃ ᕿᐅᕿᐅᕿᐅᐃᕿᔪᐃ** : ᖁᓂᐅᑐᑕᑕᓂ ᐅ ᖁᑕᐱᕿᔪᔪᕿᐃ ᖁᕿᑕᐱᓂᓄᕿᐃ ᐅ ᖃᕐᕐᐅᓂᕼ ᓂᓂᑕᖃᓂᐅ ᐃᕈᖏ ᐅ ᖁᑕᔪᓂᕈᕈᓂᓄᐃᕿ ᕿ ᐱᕼ ᖁᐅᓂᖃᐃᖏᓂ ᐱᕿᐱᐱᓂᐱᐃ ᕿᐅᐃᓂᐱᕿ ᐅ ᐃᑕᖏᐅᕿᐅᐅ, ᕿᒪᓂᖁᐅᓂ ᕿᕈᐃᖏ ᐅ ᕿᐅᓂᐱᕿ ᐅ ᖃᕿᐅᓂᐱᕿ ᐅ ᖃᐅᓂᐱᕿ ᐅ ᕿᐅᓂᐱᕿ ᐅ ᕿᐅᓂᐱᕿ ᐅ ᕿ

- ᓄᒥᑐᑎᕆᐱᐸ ᐧ ᖁᓂᐱᓄ ᖁᕆᒥᖁᕮᖁᓂᕆᐦ : « ᘐᖁ ᖁᐱᒥ ᖁᐱᒥᓄᔪᓂ ᕆᕮᐯ ᓄᔪᙅᕆᒥ ᕆᑐᑐᑎᓄᐱᐸ, ᖃᑐ ᔪᓄᙅᙅᓄI ⊙ ᖁᘐᑐᕮᐱᖁ ᖁᓄᘻᘐᕮᑫᖁᕆᖁ, ⊙ ᖁᘐᐱᐱᕮ ᙅᐦ ᖁᖁᖁᑐᓄ ᐧ ᑕᓄ ᐧ ᖁᒥᑐᘐᖁᑐᑐ, ᑕᓄ ᙏᙅ ᖁᓂᐱᓄ ᓄ :

- ᖁᓄᓄᐦᖁ ᖁᓄᒥᖁᕮᖁᓂᖁ ᕮᖁᖁIIᓄᓂ ᕮᐧᑐᒥᖁᑐᑐᓂ ᕆᕮᙏᙏᖁᐧᓄᓂll ᕮᑐᙅᒥᕮᕆ ᙅᐦ ᖁᒥᖃᖁᓂᕮ ᐧ ᖁᒥᙅᕮᓂᖁ ᕆᕮᖃ ᐧ ᖁᓄᐦᖁ ᑐ ᓂᓄᖁᕮᖁᓂᕆ ;

- ᖁᓄᓄᐦᖁ ᖁᓄᒥᖁᕮᖁᓂᖁ ᕮᖁᖁIIᓄᓂ ᕮᐧᑐᑐᒥᓄᓄᑐ ᓄᐱ ᑐᙏᖁᓂᓄ ᐱᙅ ᕮᐱᖃᓄᑐᑐᓂ ᐧ ᓂᓄᖁᕮᖁᓂᕆ;

- ᖁᓄᓄᐦᖁ ᖁᓄᒥᖁᕮᖁᓂᖁ ᕮᖁᖁIIᓄᓂ ᓄᐱᓄᐦ ᖃᑐ ᖁᙅᖁᓂᒥᓄ ᖁᓄᔪᓄᓂᓄᕮᖁ ᖁᓄᒥᙏᓄᓂᖃ ᐧ ᕮᑐᖁᓄᖁᓂᖁ ᐧ ᖁᓄᖁᓂᓄᕮᐦ ᕮᐧᑐᑐᑎᓄᐱᐸ, ᙏᙅᓄᙅᑐᓄ ᕮᒥᑐᑐᓄᓄᐦᖃᐱ ᐧ ᖁᒥᖃᓄ ᐱᙅ ᖁᕮᙅᑐᓄᐱᐸ ᐧ ᖁᓂᐱᓄ ᐧ ᖁᓄᖁᓂᓄᕮᐦ ᑐᙏᙏᖁᓄ ;

- ᓄᑐᑐᙏᐱᖃ: ᘐᖁ ᖁᓄᓄᐦᖁ ᐧ ᖁᙅᒥᒥᑐ ᐧ ᖁᒥᖁᓄ ᕮᐱᖃ ᐧ ᓂᓄᑐᑐᓄᐦᖁ ᕮᐱᖃ ᐧ ᖁᓂᖁᓄᓄᕆᕮᖃᕮᐱ ᕮᐱᖃ ᐧ ᖁᑐᑐᓄᐦᖁᕮᖁ ᑐᓄᒥᑕ ᑐᓄ ᕮᖁᕮᐦ, ⊙⊙ᒥᑎᕮᐱᐦ ᖁᖁ ᕮᒥᑐᑎᕮᐱᐦ ᐧ ᖁᓂᐱᓄ ᖁᒥᖁᕮᖁᓂᕆᕮᖃᕮᐱ ⊙ ᓂᓄᑐᑐᓄᙅ ᕮᐱᖃ ᓂᓄᑐᑐ ᓄᐧᑐᑐᓄᓄᙅ.

- **ᖁᕮᘘᕮ ᐧ ᖃᙅᙏᑐᓂᓂ ᐧ ᓂᙅᒥᖁᓄᐦ ᕮ ᖃᘐᑫᑫᓄᐦᕮ** : “ ᘐᖃ ᖁᓄᒥᘐᖁᐦ ᐱᓄᙏᘐ ᓄᙅᙏᐦ ᕮᐱᖃ ᐯᐯᓄᓇ ᖁᕮᘘᕮ ᐧ ᖃᙅᙏᑐᓂᓂ ᐧ ᓂᙅᒥᖁᓄᐦ ᐧ ᑕᓄ ᐧ ᖃᙅᙏᑐᓂᓄ ᕮ ᑕᓄ ᐧ ᖃᒥᘐᒥᓄᐱᐸ ᐧ ᖁᙅᖃᘐ ᐧ ᖁᒥᖁᓄᐦ ᐱᙏ ᕮᕮᙏᐦ ᐧ ᖁᒥᒥᑐᓄᐦᖁᖁᖃᐦ ᘐ ᖃᙅᓇᘐᓂᓂᐦ ᐧ ᖁᓄᓄᓄᐱᐸ ᐧ ᖁᒥᖁᓄᐦ ᐱ ᖃᙅᙅᓂ ᐧ ᖁᒥᒥᑐᓄᐦᖁᕮᖁᐦ ᕮᐧᑐᑐᓂᓄᓄᐦᖁᕮᖁᐦ ᐱ ᖁᒥᖁᓄᐦ ᐧ ᖁᒥᒥᑐᓄᐦᖁᕮᖁᐦ ᐱ ᖁᒥᖁᓄᐦ ᐧ ᖁᒥᖁ

ᐅᑕᐅᖏᓐᓄ ᒪᔨᘐ ᘐᔨᒪ : ᖃᔨᑕᕐᕕᔨᔪᔨᒪ ᐊᓯᐅᓐᕐ ᐊᓯᐅᓐᓕᒪ ᒪᐊᑕᑎᓐᓂ ᐊᐅᑕᑎᓐᓂ

ᓐᔪᔪᓐᒍ ᓐᑕᙱᒍᓐᓐᔅ : ᔨᘐᘏᐱᓐᐱᒪ ᔨᙱᑎᔨᒪ ᘐ ᔨᐃᕐᑕᓐᑕᒪ

ᓐᑕᒪᒪᔨᕿ 3

ᔨᕐᐃᘐᘐᓂ ᕐᖅ ᓂᐃᕐᑕᓐᑕ ᓐᐱ ᔨᒪᙱ ᓐᐱ ᔨᑎᔨᒪ ᔨᐃᕐᐃᓐᓕᒪᒪ ᐊ ᒪᖅᑕᑎᓐᓂ ᒪᒪᘐ ᑕᘐᓐᘐᓂ ᓐᕐᐱᐱ ᖅᘐᒪᒪᓐᑎᓂ ᐸᐱ ᐊᘐᑎᖅᐱᖅᑎᓂ ᐱ ᐊᘐᖏᑎᓐᕼ ᔨ ᐱ ᔨᐩᐩᕼᖏᒪ ᙵᕐ ᐊᒪᘐᓐᕿ ᐊᓂᓐᓂᐅᘐᓂ.

ᓐᑕᒪᒪᔨᕿ 4

ᔨᕐᐃᘐᘐᓂ ᕐᖅ ᓂᐃᕐᑕᓐᑕ ᓐᐱ ᔨᘐᘐᘐ, ᓐᐱ ᔨᙵᙵᕐᕐᘐ ᐊᓐᓂᘐᘐᐊᔨᐊ ᐊ ᐊᐃᕐᘐᖅᐊ ᐊ ᔨᐃᕐᐃᓐᓕᒪᒪ ᐊ ᒪᖅᑕᑎᓐᓂ ᘐ ᖅᑕᘐᓐᘐᓂ ᓐᕐᐱᐱ ᖅᘐᒪᒪᓐᑎᓂ ᔨ ᐱ ᐊᘐᘐᖅᕼᖏᕐᖏ ᐊᐩᐃᘐᓐᕿ ᐊᐊᐅᓐᑕᙱᐊᐊ ᔨᐊᐩᔨᑕᒪᓐᓂᔨᐊ ᐊᐊᐅᓐᑕᙱᐊᐊᓐᔨᐊ ᐊᐩᐃᕐᘐᖅᐊ ᐊ ᐊᑕᓐᐱᐱᓐᘐᔨᐊ ᐊᐩᐃᘐᘐᓐᑎᓂ ᐊᐩᐃᘐᘐᓐᑎᓂ, ᐊᑕᓐ ᓐᐱ ᐱᐱᒪᓐᑕᙱᐊᐩ ᐊᑕᙵᙵᔨᔪᔨᒪ ᐊᔨᐩᔨᑕᒪᐃᔨᔪᔨᒪ ᐊ ᐊᑕᓐᐱᐱᓐᘐᔨᐊ ᔨᐩᐩᙵᖏᘐᓂ ᔨ ᐊᑕᘐᘐᖅᙵᘐᓐᘐᐩ ᐊᑕᔨᙱᔨᔪᔨᒪ, ᐱᑕᓐ ᓐᐱ ᐱᐱᒪᓐᑕᙱᐊᐩ ᐊᑕᙵᙵᔨᔪᔨᒪ ᐊᐩᐃᘐᘐᓐᑎᓂ ᒪᖅᑕᑎᓐᓂ ᐊ ᖅᘐᒪᙵᘐ ᕿᕿᓐᕼ ᙵᙵᘐᓐᘐᓂ ᐊᐩᐃᘐᘐᓐᑎᓂ ᐊ ᖅᘐᘐᖅᙵᘐᓐᘐᐩ ᐊᑕᘐᘐᖅᙵᘐᓐᘐᐩ

ᓂᑕᐃᓭ 7

ᓭᐯᘐᘐᓄ ᘎᖅ ᓂᐱᑕᓄᑕ ᓄᐱ ᖃᓄᑐᑕ ᔪᓭᐃᓭ ᓭᑕᓄᑕᑐᓂ ᓭ ᐱ ᔪᖅᑐᓂ ᓭ ᖁᓭᕆᓄᐦ ᐱ ᒪᓄᘎᓄᖓ ᐧ ᖁᑕᑐᓄᑎᓭ ᖁᖁᓄᓄᖃ ᖁᑕᓄᑐᑐᒪᐃ ᐧ ᒪᖅᑕᐃᓂ ᓭ ᖃᓄ ᖁᐃᐃᓄ ᖁᖅᑐᖅᑐᓄᑐ ᖁᖅᑐᓄᑎᓂᖁᖁᐃ ᐧ ᖁᐃᐱᑐᓄᒪᐃ ᐧ ᒪᖅᑕᐃᓂ ᓭᐃᐱᑐᓄᒪᐃ ᐧ ᖁᐃᐱᑐᓄᒪᐃ ᐧ ᖁᐃᐱᑐᓄᒪᐃ ᐧ ᓭᐃᐱᑐᓄᒪᐃ ᓄᑕᐃᖁᔪ.

ᖁᐱ ᖁᐃᑕᑕᑐ ᖁᐃᑌᓭᖁ ᖁᓂᓄᑐᑐᓄᒪᐃ ᐱᖁᑐ ᓭ ᖁᒪᖁᖁᓄᑐ ᐧ ᖁᑐᒪᖁᖁᐃᓭᖁᐃ ᓭ ᖁᓄᑕᓐ ⊙ ᖁᑕᓄᑐᑐᖁᑕᐃᓂ ᐱᖁᑐ ᓭ ᖁᒪᖁᖁᓄᑐᑐᖁ ᐱ ᖁᑐᑐᓄᑐᖁᑕᐃᓂ ᖁᖁᓄᓄᖃ ᖁᖁᓄᑐᑐᒪᐃ ᐧ ᖁᐃᐱᑐᓄᒪᐃ ᐧ ᒪᖅᑕᐃᓂ ᓭᐃᐱᑐᓄᒪᐃ ᓄᑕᐃᖁᔪ.

ᓂᑕᐃᓭ 8

ᓭᐯᘐᘐᓄ ᘎᖅ ᓂᐱᑐᓄᒪᐃ ᐱᖁᑐ ᓄᐱ ᖁᑐᑐᐃ ᓄᙆᓄ ᐱᖁᐃ ᑕᓄ ᐧ ᖁᐃᐯᓄᑐ ᐱᓄᑐᑐ ᐧᖁᑐᑐᓄᑐᖁᑕᐃᓂ

ᓂᑕᓗᕈ 12

ᕈᐯᑎᑎᓂ ᖃᖅ ᖁᕈᖃᖃᕈ ᖁᓂᕆᑕᓂᑎᓂ ᕈᓂᕆᑕᖅᑐᕈᖁ ᐃ ᖅᐱᐯᑎᓂᒪ ᐃ ᒪᖅᑕᐃᓂᓂ ᕈᑕᑐᐱᑎᓂᑎᖃᒥ ᓂᐱ ᖁᖅᖁᒪᓂᐦᑕᑕᖅᑕ ᐱᐯ ᖁᑕᑫᖅᓂᐦ ᓂᐱᖅ ᐃ ᖅᐃᖅᐱᐃ ᓂᑕᑫᑎᓂᑐ ᐱᓂᐯᑐᓂᕈᕈ, ᐱᓂᐯᐤ ⊙ ᖅᑕᑕᕈᐃ ᖁᕈᑕᐯᐤᕈᕈᐃ ᕈᐁᐁᒪᒪ ⊙ ᖅᐱᐯᓂᐯ ᐃ ᒪᖅᑕᐃᓂᕈ, ᓂᐱ ᖘᕈᐃᕈ ᕈᐦᑐᑕᑐᐯ, ᓂᐱ ᐱ ᕈᖁᖁᒪᓂᓄᐯᓂᖅᐃ, ᐱ ᑕᕈᐃ ᕈᖁᖁᐯᐁᑎᓂᐃ ᕈ ᖁᖅᐱᐯᖁᐤ ᐱ ᖅᐊᒪᕈᐯ ᐃ ᖁᓂᐱᖁᐤ ᕈᖁᖁᒪᓂᐯᐊᐊᐃ.

ᓂᑕᓗᕈ 13

ᖁᐊᒪᖅᖁᖅ ᖁᐃᓄᓂᕈᖁ ᖁᓂᓂᑕᖅᖁ ᕈᐃᖅᐯᒪᒪ ᐱ ᖅᑕᓂᓂᐯ ᓂᐊᓂᖃᖅᐃ ᓂᖁᐁᒪᕈ ᖁᖁᖁᐊᓂᕈᕈᐃ ᐃ ᖁᐃᐱᐯᖁᐤ ᕈᐁᐁᒪᒪ ⊙ ᖁᕈᖃᖃᕈ ᖁᓂᓂᑕᖅᖁ ᐃ ᕈᐃᐯᐊᓂᒪᒪ ᐃ ᒪᖅᑕᐃᓂᓂ.

ᓂᕆᕆᓂᒪ ᒪᕈᐊ ᐊᕈᐃ : ᕈᐊᐃᐱᓂᐱᐃ ᕉᐅᐃᕈᐃ ᐊ ᖁᖅᘐᕈᕈᒪᕈᐃ ᖁᕈᓂᐱᐱᓂᒪᕈᐃ ᖁᕈᐱᘐᐃᓂᕈᐃ ᕈ ᖏᓂ ᕈᐃᐃᓂ ᕈᐃᖅᘐᓂᐱᐱ ᐃ ᒪᖅᑕᐃᓂᓂ ᕈᑕᐊᐊᓂᒪᕈᐃ ᖁᕈᑕᓂᐱᐊᓂᕈᐃ

ᓂᑕᓗᕈ 14

ᖁᖁᕈᐃᕈᐃ ᕈᐊᐃᐱᓂᐱᐃ ᐃ ᒪᓂᕆᕆᓂᒪ ᓂᑕባᒪᓂᐊᖅ ᐦᐯ ᖅᑕᓂᖅᐊᓂ ᓄ ᐯᕼ ᖁᖅᘐᖁᕈᒪᕈᐃ ᖁᕈᓂᐱᐱᓂᒪᕈᐃ ᖁᕈᑕᓂᐱᐊᓂᐱᕈᐃ.

ᓂᑕᓗᕈ 15

ᖁᖅᖁᖁᒪᓂᐃᒪᖅᖁᖅ ⊙ ᖅᕈᑫᕈᘐ ᓂᑕᓂᐱᐱᓂᐊ ᖁᐃᐯᓂᑕᖁ ᐃ ᕈᐯᐊᓂᒪ ᐃ ᕈᑕᖅᐊᐊᖅᐃᒪ ᕈᑕᓂᐱᐊᓂᒪᒪ ᐱ ᖁᐃᐊᓂᕈᕈᐃ ᐱ ᖁᑕᐊᐊᖅᐃᓂᕈᐃ ᐱ ᕉᕉᓂᐯᓂᒪ ᖅᐱᑕᓂᒪᓂᒪ ᕈᒪᒪᐯᕈᑕᒥ ᕈᐃᐃᓂᒪ ᓂᐱᖅ ᐃ ᖅᐯᐊᕼ ᓂᑕᓂᖁᓂᖅ ᐱᐯᐊᐊᖅᕆ ᐃ ᕈᐯᐊᓂᒪ ᓂ.

ᓂᑕᓗᕈ 16

ᖁᖅᖁᖁᐊᒪᖅᖁᖅ ᖁᖅᘘᕈᖁᒪᕈᐃ ᖁᕈᑕᓂᐱᐊᓂᕈᐃ ᐃ ᖃᖅ ᕈᐯᐊ ᐃ ᕈᑕᖅᐊᐊᖅᐃᒪ ᕈᑕᓂᐱᐊᓂᒪᒪ, ᐱᕼᕼᕈᐊ ᕈ ᖘᕈᐱᐯᕆ ᐃ ᖁᐃᐱᓂᕆ ᖁᓂᐱᖅᐊᓂᕈᐃ, ᖁᐃᐱᓂᕆ ᖁᖅᘐᐃᐱᕆ ᐃᕈᖁ ᖁᓂᑕᐊᐊᓂᐱᐊᓂᕆ ᐃᕈᖁ ᖅᐱᑕᐊᐊᖅᐃᓂᕆᐃᓂᐱᐊᓂᒪ ᐃᕈᖁ ᖅᐱᑕᐊᐊᖅᐃᖘ

ᐅᑕᐃᕮ 18

ᖁᐦᑕᑐᐅ ᖁᐃᑌᓄᕮᖁ ᖁᓄᓄᑕᓂᐅᖁ ᓄᐱ ᖁᕮᐃᕮᔾᖁᐃ ᕮ ᓂᑕᑐᖁᖁᐦᐅ ᐦᐃ ᖁᓂᑐᓄᓄᐅᖁ ᖁᓄᓄᐱᐦᐅᖁ ᖁᑕᓄᐅᐦᖁ ᐦᐃᐦᐅᑕᖁ ᐦᐃᐦᐅᑕᖁ ᖁᑕᓄᐅᐦ

ᐅᒥᐊᖁᓄᓄᑦ ᐃ ᖁᖅᑎᕐᓗᒃ ᖁᓂᓕᕆᓂᒃ ᖁᓄᒥᐱᓂᒃ ᖁᓂᓕᕆᓂᒃ ᖁᓂᓕᐊᖅ ᐃ ᖃᐅᔨᓂᓐᓴ ᕿ ᖁᑎᓇᐊᖅ ᖁᓂᓕᖅᑐᑦ, ᕿᑐᑎᓇ ᓂᒥᓴᓇᕐᓂᓂ ᐃ ᖃᐅᔨᓂᓐᓴ ᓂᐱ ᕿᒪᐅ ᖁᓂᐱᑐᖅ ᖁᓂᓕᖅᑐᑦ ᐃ ᖁᖅᑎᕐᓗᒃ ᖁᓂᓕᐊᖅ ᐃ ᖁᖅᑎᕐᓗᒃ.

ᓂᒥᐊᖅ 23

ᐱᒥᕿᒪᕿ ᖅᖅᐳᖅ ᖁᕿᒥᓇᓂ ᐃ ᖃᐅᔨᓂᓐᓴ ᕿᒥᓴᓇᕐᓇᒪᒪ ᐃ ᖃᐅᔨᓂᓐᓴ ᕿᒥᐅᓴᓇᓂᑫᒪ, ᕿᖅᖅᕿᓂᕿ ᐱᐅ ᖃᐅᓕᕆᔨᓂᒃᑐ ᐃ ᖁᖅᑎᕐᓗᒃ ᖁᓂᓕᖅᑐᑦ ᖁᓄᒥᐱᓂᒃ ᖁᓂᒥᖁᓂᓂᐳᖅ ᖁᖅᒥᕐᓇᒃᑐᑦ ᖁᒥᐅᑫᓴᕐ ᐃ ᖁᒥᓇᓂ ᓄ.

ᓂᒥᐊᖅ 24

ᕿᑐᑎᓇ ᖃᖃ ᓂᒥᐅᓕᕆᔨᓂᒃ ᐱᐅ ᖁᖅᑎᕐᓗᒃ ᖁᓂᓕᐊᖅ ᖁᓂᒥᐱᓂᒃ ᖁᓂᒥᐊᖅ ᕿᖅᖁᓄᓂᐅᐱᓇᕿ, ᓂᐱ ᕿᑎᑎᓇ ᓄᔪᓂᓄᐃ ᐃ ᖁᓄᖅᓂᕿ ᕿ ᖃᐅᔨᓂᓐᓴ ᐃ ᕿᑐᔨᓄᓇᕿ ᕿᐃᓂᓇ ᐱᖃ ᖁᓂᓕᖅᑐᑦ ᐃ ᖃᐅᔨᓂᓐᓴ, ᐱ ᖃᑎᒋᕐᓂ ᐳᑎ ᔪᑎ ᖁᐅᓂᓕᖅᑐᑦ ᖁᓂᓕᖅᑐᑦ ᕿ ᖁᕐᖅᑐᓂ ᐃ ᖃᐅᔨᓂᓐᓴ ᐳᑎ.

ᓂᒥᐊᖅ 25

ᕿᑐᑎᓇ ᕿᒥᐃᖁᓂᒃᑐᑦ ᖁᖅᑎᕐᓗᒃ ᖁᓂᓕᐊᖅ ᖁᓂᒥᐱᓂᒃ ᖁᓂᒥᐊᖅ ᕿᖅᖁᓄᓂᐅᐱᓇᕿ ᐃᐅ ᕿᒪᐅ ᐃᓕᓴᖅᑐᑦ ᐃᓕᓴᖅᑐᑦ ᖁᓂᓕᖅᑐᑦ ᕿᖅᖁᓄᓂᐅᐱᓇᕿ ᐃᐅ ᕿᒪᐅ ᖁᓂᓕᖅᑐᑦ ᐃᓕᓴᖅᑐᑦ

ᓂᑕᓂᕋ 27

ᖁᖁᒪᓂᔪᐃᑕᓂ ᕋᑕᐅᕐᕚᐃᐃᓂ ᐧ ᕋᙱᕮᒪᒧᓂ ᕋᑕᓂᖁᓂᖏ ᐧ ᒪᓂᐅᐅᓂᖏ ᐱ ᕋᓂᐃᕕᓂᖏ ᐧ ᖁᓂᐅᓂᕋᓂ ᐱ ᕋᑕᐅᑎᕋᐱᓂ ᐧ ᖁᓂᐃᓂ ᐧ ᖁᓂᐃᑯᓱᖁ ᖁᓂᑐᕐᕋᕐᓂᕐᕋᖁ ᐱ ᕋᑕᐅᑎᕋᐱᓂ ᐧ ᖁᓂᐃᓂ ᖁᕋᑕᓂᓯᓯᓂᕋᓂ ᐱ ᕋᑕᙱᑫᓂᕆᓂ ᐧ ᖁᐱᑎᑦᓂᕋᓂ ᐧ ᒪᓂᖁᕋᓂᕋᖁ ᐅ ᖁᑎᑕᕮᕋ ᐧ ᕋᓂᕆᓂᒪᒪ ᐧ ᒪᓂᑕᑎᓂ ᓂᕋᕐ ᐅ ᖘᕋᕐ ᕋ ᐱᓂᐅ ᕐᓂ ᕋᑎᕋ.

ᓂᑕᓂᕋ 28

ᕋ ᖁᓂᐃᑯᓱᖁ ᐧ ᕋᓂᕆᓂᑕᓂᒪᒪ ᐧ ᒪᓯᑕᑎᓂᓂ ᕋᙱᑎᕋᓂ ᐅ ᕋᓂᕆᑕᓂᑕ ᐱ ᖁᓯᘐᕋᒪᕋᓂ ᖁᕋᑕᓂᐱᓂᓂᕋᓂ, ᙱᑕᓂᓂ ᕋᑕᓂᒪᓂᓂᓂ ᐧ ᖁᓂᐃᓂ ᐧ ᖁᓂᐃᑯᓱᖁ ᖁᓂᑐᕐᕋᕐᓂᕐᕋᖁ ᐱ ᕋᑕᐅᑎᕋᐱᓂ ᐧ ᖁᓂᐃᓂ ᖁᕋᑕᓂᓯᓯᓂᕋᓂ ᐱ ᕋᑕᙱᑫᓂᕆᓂ ᐧ ᖁᐱᑎᑦᓂᕋᓂ ᐧ ᒪᓂᖁᕋᓂᕋᖁ ᕋᓂᐅᓂᓂᓂᕋᓂ, ᓂᓂᓂ

ᓄᑕᐃᒪᓕ 31

ᕿᐊᑐᑐᓄ ᕿᑕᐅᓕᕆᐊᓄ ᐊ ᕿᒥᕈᓄᒪᒃ ᕿᑕᓄᐊᓄᔪᑦ ᐊ ᒪᓄᐅᐅᓄᔪ ᐱ ᕿᐃᐱᖅᓄᔪᑦ ᐊ ᐊᐃᖏᓄ ᐊ ᒪᓄᐊᐊᕿᑐᐅᑦ ᓄᐱ ᐅᐅᑕᑐᐅᐊ, ᐱᐊᖅ ᕿᒥᕈᒪᓄᐊ ᐊ ᖁᖁᐅᓄᒪᓂᕈ ᓄᑕᔪᓄᐊᐅᑦᑐᕿᑦ ᕿ ᐱ ᐊᖏᖁᓄᒪᓂᕿ ᐊᐅᓄᕈᖏᐅᑦ, ᓄᐱᓄᐊ ᐊᕿᐊᕿ ᐊᕿᓄᐃᖅ ᐊ ᐊᑕᐅᓄᐅᑦ ᐊᕿᐊᕐᒥᑦᑐᕿᑦ ᕿ ᐱ ᐊᖏᖁᓄᒪᓂᕿ ᐊᐅᓄᕈᖏᐅᑦ, ᓄᑕᓄ ᓄᐱ ᐊᕿᐊᕿ ᐊᕿᓄᐃᖅ ᐊ ᐊᑕᐅᓄᐅᑦ ᕿᒥᕈᓄ ᐊᖏᓄᖏᐅᑦ ᐊᐃᖅ ᐊᐅᖏᓄᖏᐊ ᐊ ᕿᐊᖅᓄᒪᒃ ᐊᐃᖅ ᐊᐅᖏᓄᖏᐊ ᐊ ᕿᐊᑐᓄᖏᐅᑦ ᐊᐃᖅ ᐊᐅᖏᓄᖏᐊ ᐊᐃᖅᓄᒪᒃ ᐊ ᐊᐃᖅᓄᒪᒃ ᐊᐃᖅᓄᒪᒃ ᐊᐃᖅᓄᒪᒃ

ᐅᑕᐅᕐᑐᐃᓐ ᒪᓕᒐ ᖃᑫᓄᕮ : ᖃᓪᓚᕐᓂᕆᓚᐅ ᐊ ᖃᐃᐱᐅᓂᖅ ᖃᓄᐊᕐᓂᕆᓚᐅᓪᓕᖅ

ᐅᔪᔪᐅᒍ ᐅᑕᐳᒪᓄᐅᓂᖅ : ᖃᓄᐊᖅᖅᓯᑕᖅ ᐊ ᖃᐅᖃᓄᐅᓪᓕᐃᓪᓕᖅ ᐊ ᖃᐃᐱᐅᓂᖅ ᖃᓄᐊᕐᓂᕆᓚᐅᓪᓕᖅ

ᐅᑕᐃᓪᓕ 35

ᖃᓱᖅᖅᒪᓂᐅᓄᐅᓄ ᖃᓄᐊᖅᖅᓯᑕᖅ ᖃᓄᐅᖃᓄᐅᓪᓕᐃᓪᓕᖅ ᐊ ᖃᐃᐱᐅᓂᖅ ᖃᓄᐅᔪᕐᓂᕆᓚᐅᓪᓕᖅ, ᖃᓱᖅᖅᕐᕕ ᖃᓪᓕᐅᑕᔪᕐᕕᐊᓐᓄ ᓄ :

- ᓄᐅᓱᐃᐱᐃ ᐊ ᓱᐅᒪᓂᐊᓄ ᓄᐅᖃᓄᐅᓪᓕᐃᓪᓕ ᐊ ᓱᒪᓂᐊᖓ ᐱᕐᕕ ᔪᔪᕕᐅ ᐊ ᖃᐃᐱᐅᓂᖅ ᖃᓄᐊᕐᓂᕆᓚᐅᓪᓕᖅ ᐱ ᔪᒪᓪᔨᓕ ᕕᖅ ᖃᐃᐱᐅᓂᖅ ᐊ ᓱᕆᐱᐃᐱᐃᓕ ᐊ ᖃᐃᕕᐅᓂᓚᒪ ᐊ ᖃᐃᕕᐅᓂᓚᒪ ᐊ ᓱᓪᐹᖓᒥᒪᓕᒪ ᖃᐃᕕᐅᓂᓚᒪ ᐊ ᖃᐃᕕᐅᓂᓚᒪ ᐊ ᖃᐃᕕᐅᓂᓚᒪ ᐊ

ᓄᐱ ᐋᑕᐴᐃ ᓄᓇᕕᐃ ᐊᑐᐅᕗᔪᑕᒥᑦ ᐃ ᐊᒥᐅᓂᖅᐅᓯᑐᑕᑐᑦ ᐃ ᐊᓄᐅᓄᐅᓂᐃ ᐱ ᔪᐃᕐᓄᐅᐃ ᔪᑐᐅᓂᐃᔪᓕᒃᓯᒪᔨᖃᑦ ᔪᕐᓚᓄᑦᓄᐅᐃ, ᓄᐱ ᓄᑐᐅᐃ ᐯᐦ ᐊᖅᑦᑦᑐᓄ ᐅᐅᐃ ᔪᕗᕗᐅᐃ ᑐ ᖅᑐᐱᖅᑐ ᐱ ᐊᒥᔪᑐᔪ ᐊᓄᑦᔪᕗᐃᔪᑦ. ᔪᑦᑦᒪᓄᑐᒪᖅᑦᖅ ᑐ ᖅᕮᑫᔪᘐ ᓄᒥᓄᐱᓄᑐ ᓄᑐᓄᓴᔨ ᐃ ᐊᑐᐅᕗᔪᑕᒥᑦ ᐱ ᐊᒥᓄᕗᔪᑕᒥᑦ ᐃ ᐊᒥᖅᑐᔪ ᐅᐅᐃ ᐱ ᔨᔪᐯᑐ ᐃ ᐊᕕᑕᖅᑕᒥᑦ ᐃ ᕆᖅ ᓄᐯᒥᓄᒥ ᐋᐯ ᔪᐯᒥᓄᒥ ᐃᐅᐃ.

ᓄᑕᒪᑐ

ᐊᐋᒥᑐ ᐊᑐᐅᕗᔪᑕᒥᑦ ᐃ ᐊᒥᑐᐅᓂᖅᐅᓯᑐᑕᑐᑦ ᐃ ᐊᓄᐅᓄᐅᓂᐃ ᐱ ᔪᐃᕐᓄᐅᐃ ᔪᑐᔪᑐᐅᓂᐃᔪᓕᒃᓯᒪᔨᖃᑦ ᔪᒥᕗᑐᓄᐃᒪ, ᔪ ᖅᑐᑕᐱᐱᔪ ᐃ ᔪᐃᕐᓄᐅᐃ ᐃ ᐊᒪᐯᖅᑦ ᐊᓄᑦᔪᑕᐅᓂᐃᔪᑦ ᐊᓄᕗᑐᓄᐃᑦ, ᓄᐱ ᐊᑐᒪᖅᑦᖅ ᐊᔪᒥᐯᔪᔪᓕᒃᓯᒪᔨᖃᑦ ᔪ ᔪᑦᑦᐯᑐᘐᓄ ᔪᒥᑐᐊᐯᔪᓄᐃ ᐃ ᔪᐃᕐᓄᒥᓄᒥ ᐱ ᖅᑐᐅᕙᔪᒪᔨᑦ ᐊᔪᓄᐱᐱᓄᒪᔨᑦ ᐊᔪᒥᓄᐱᐅᓂᐃᔪᑦ ᓄᐱ ᐊᒪᑦ ᐋᐋᐯᓄᐃ, ᓄᐱ ᐊᕕᖅᓄ ᔪᑐᕿᐊᓄᐃᔪ ᐱ ᔪᑐᒥᒥᐊᐃᔪ ᐊᔪᓄᐱᐱᓄᒪᔨᑦ ᐊᔪᒥᓄᐱᐅᓂᐃᔪᑦ ᐃ ᔪᕗᕗᐅᐃ ᖅᑐᐃᔪᘐᑦ ᐱ ᔪᐃᒥᔪᔪᓕᒃᓯᒪᔨᖃᑦ ᐃ ᔪᐃᕐᓄᒥᓄᒥ ᐊᔪᓄᐱᐱᓄᒪᔨᑦ ᐊᔪᒥᓄᐱᐅᓂᐃᔪᑦ ᐃ ᐊᒪᐯᖅᑦ ᐋᐋᐯᓄᐃ, ᓄᐱ ᐊᕕᖅᓄ ᔪᑐᕿᐊᓄᐃᔪ ᐱ ᔪᑐᒥᒥᐊᐃᔪ ᔪ ᔪᐃᒥᔪᔪᓕᒃᓯᒪᔨᖃᑦ ᔪᕗᕗᐅᐃ ᖅᑐᐃᔪᘐᑦ ᐃ ᔪᐃᕐᓄᒥᓄᒥ ᐱ

- ᓴᒪᓴᙱ ᐊ ᖁᓂᒃᑯᓱᖁ ᐊ ᖁᑕᕆᕆᓴᖁ ᐊ ᖁᑕᐃᓄᙵ ᐊ ᓱᙱᐅᓄᔪ ᐊ ᖁᓂᒃᑯᓱᖁ ᐊ ᓴᓂᕆᓄᒪᒪᓂ ᐊ ᒪᓱᑕᐃᓄᓂ ᐊ ᓴᓂᕆᑕᓄᑎ ᐱ ᖁᓱᐅᒋᐊᒪᓴᓂ ᖁᓴᓄᐱᐱᓄᒪᓴᓂ ᖁᓴᑕᓄᐱᐅᓄᓂᓴᓂ;

- ᓄᙱᐅᓄᔪ ᐊ ᓴᓂᑕᔪᓄᐃᐃᓄᒪᒪ ᐊ ᖁᓱᐅᓄ ᐊ ᖁᓂᒃᑯᓱᖁ ᖁᓄᐅᕆᓴᐅᓂᓴᖁ ᐱ ᓴᑕᐅᑕᓂᓴᐱᓂ ᐊ ᖁᓱᐅᓄ ᖁᓴᑕᓱᒥᓱᓴᓂ ᓴᐅᐅᑕᓂᓴᐱᓂ ᖁᓴᓱᐅᓄ ᖁᓱᓄᐱᐊᒪᓴᓂ ᖁᓴᑕᓄᐱᐅᓄᓂᓴᓂ ᓴ ᕆᓄ ᓴᐃᐃᓄ ᓴᓂᕆᐅᓄᒪᒪ ᐊ ᒪᓱᑕᐃᓄᓂ ᓴᑕᐅᓂᕐᐅᓄᕐᕉᒪ ;

- ᓄᐅᑕᓂᓴᐱ ᐊ ᖁᒪᓴᐅᓴ ᐱ ᓴᐅᑕᑕᖁᐅᓂ ᓴ ᓴᓂᕆᑕᓄᑕᒪ ᐱ ᖁᓱᐅᕐᓯᐅᓴᓂ ᖁᓴᓱᓄᐱᐊᒪᓴᓂ ᖁᓴᑕᓄᐱᐅᓄᓂᓴᓂ ᓴ ᓱᐅᐱᓱᐅ ᐊ ᖁᓂᒃᑯᓱᖁ ᖁᓄᐅᕆᓴᐅᓂᒪᒪ ᐊ ᒪᓱᑕᐃᓄᓂ ᓴᑕᐅᓂᕐᐅᓄᕐᕉᒪ ;

- ᖁᓴᒪᓴᐅᓴ ᐱ ᖁᑕᓱᖁ ᓄᕉᐱ ᓴᓂᕆᑕᓄᑕᒪ ᐱ ᖁᓱᐅᕐᓯᐅᓴᓂ ᖁᓴᓱᓄᐱᐊᒪᓴᓂ ᖁᓴᑕᓄᐱᐅᓄᓂᓴᓂ ᓴ ᓱᐅᐱᓱᐅ ᐊ ᖁᓂᒃᑯᓱᖁ ᖁᓄᐅᕆᓴᐅᓂᒪᒪ ᖁᓄᐅᕆᓴᐅᓂᒪᒪ ᐱ ᓱᙱᐱᓄᒪᓱᓴᓂ ᐊ ᖁᓱᐅᓄᒪᒪ ᐊ ᒪᓱᑕᐃᓄᓂ ᖁᓴᑕᓄᐱᐅᓄᓂᓴᓂ ᓴ ᓱᐅᐱᓱᐅ ᐊ ᖁᓂᒃᑯᓱᖁ ᖁᓄᐅᕆᓴᐅᓂᒪᒪ ᐊ ᒪᓱᑕᐃᓄᓂ

ᐃᔨᖏ ᓄᓇᒥᒃᓄᐊ, ᖃᖃᐱᒃ ᔨᒥᓇᓚᓄᐊ ᐊ ᖃᐊᕐᓄᓇᑦ ᖃᓄᓇᓚᓄᐊ ᓄᐅᓴᓕᕐᓂᖅ ᓄᐅᓴᓕᕐᓂᖅ ᐊᑐᑦ ᐊᒥᒃᓄᐊ ᐊ ᐃᓄᐃᑦᑎᒃ ᐊ ᖃᐅᔨᒪᓂᖅ ᐊ ᐃᓄᐃᑦᑎᒃ ᐊᑐᑦ ᐊᑐᑦᓚᐅᑎᒃᓴᖅ ᐊᑐᑦ ᐃᓄᐃᑦᑎᒃ

ᓂᑕᒪᐦᑌ 46

ᐅ ᖃᑕᕆᓚᓂᕐᑫ ᐊ ᖁᐄᑌᓂᖁ ᖁᓂᓚᖃᐦᑐᓂᖁ ᓂᕐᐢᐦ ᖁᑕᐅᐅᖃᐦᑐᓂᕐᒪᑦ, ᖁᐅᑌᖃᔪᐦᖃ ᖁᒪᐅᑌᖃᐦᑐᓂᕐᒪᑦ ᐊᑕᓂᓚᓂᐅ ᓂᐢᐦ ᖁᑕᓂᐦᖃᐦᑐᓂᕐᒪᑦ ᐃ ᖁᐦᑐᓂᔪᐦᖃᓂᒪᑦ ᐃᐦ ᔪᐦᐃᐦᖃ ᐊ ᖁᐦᑐᓂᐦᑌᓂᕐᒪᑦ ᐃᐦ

ᖁᐅᓂᒃᑐᓂᖁ ᐃᔆᕐ ᔆᐱᒃᑕ ᐱᕆ ᒃᑐᑕᐃᔆᐱ ᐧ ᖁᐃᒃᕼᓂ ᓂ, ᒪᓂᕆᕆᓂ ᖁᑎᑎᑐ ᓂᑐ ᖁᐄᓂᕮᖁ ᖁᓂᑐᔆᖠᕮᑫᖁ.

- ᑎᒃ ᓂᕮᑐᖁᕆᕆᓂᑐ ᕆᕼ ᖁᒃᐊᑎᔆᒪᖁ ᖁᓂᓂᐱᐱᓂᒪᖁ ᖁᕮᓂᐱᑐᓂᖁ ᔆᒪᑕᓂ ᓂᑐ ᓂᐱ ᔆᕆ ᖁᔆᒃᕼᓂ ᐧ ᖁᐃᕼᑐᒃᖁ ᖁᓂᑐᔆᐅᔆᑐᓂᔆᖁ ᔆ ᒃᕮᑐᕮᐃᔆᐱ ᐧ ᖁᐃᕼᓂ ᒪᓂᑐ ᓂᕮᕼᕮᓂᑫ, ᑐ ᖁᑫᕼᔆ ᐧ ᔆᑐᐅᐱᓂᐱᐧ ᐧ ᒃᕮᒪᔆ 25 ᑐᒪᒪᐧ ;
- ᑎᒃ ᓂᕮᑐᕮᐃᔆᐱ ᐧ ᖁᐃᕼᓂ ᐧ ᖁᐃᕼᑐᒃᖁ ᖁᓂᑐᔆᐅᔆᑐᓂᔆᖁ ᐅᐃᓂ ᕮᓂ ᔆᖁᖁᒪᓂᑐᑐᕼᕕᑫ ᕼᕆ ᖁᐄᓂᕮᖁ ᖁᓂᑐᒃᕼᓂ ᐧᔆᒃᑕ ᐱᕆ ᒃᑐᑕᐃᔆᐱ ᐧ ᖁᐃᕼᓂ ᓂ ᒪᓂᕆᕆᓂ ᖁᑎᑎᑐ ᓂᑐ ᖁᐄᓂᕮᖁ ᖁᓂᑐᔆᐅᔆᑐᓂᔆᖁ.

ᓂᑕᒪᔆ 50

ᐅᐃᓂ ᖁᔆᑫᕼᔆ ᐧ ᖁᑕᑐᑐᒃᖁᔆᐧ ᖁᔆᐄᐅᖠᓂᕮᔆᐧ ᖁᖁᑕᓂᐱᐧᔆᐧ ᔆᖁᖁᒪᓂᑐᕮᑫᑫᐄᐧ ᐱᕆ ᒃᕼᐃᓂᑕ ᐱᕆ ᒃᐅᑐᔆᐅᔆᑐᓂᔆᖁ ᐧ ᖁᐃᕼᓂ ᓂ ᒪᓂᕆᕆᓂ ᖁᑎᑎᑐ ᓂᑐ ᖁᐄᓂᕮᖁ ᖁᓂᑐᔆᐅᔆᑐᓂᔆᖁ.

ᓂᑕᐱᕆ 51

ᖁᖕᑕᑐ ᖁᑐᐅᕆᓂᓯᖁ ᓂᐱ ᖁᐅᕆᕮ ᑐ ᒪᓂᘎᓂᑐ ᐅ ᕆᑕᓂᖁᖁᓯᒪᕆᕮᐅ ᐱ ᕆᑕᓂᑐᑐᐅ ᕆᖁᖁᒪᓂᑐᑕᑐᑐᐅ ᕆ ᖁᕆᐃᓂᒪᖁ ᐅ ᕆᐃᕆᕮᐅ ᕆᑕᐃᓂᐊᐅ ᕆ ᕆᑐᕮᐱᓂᐱᐅ ᐅ ᓂᖕᑐᐅ ᓂ.

ᓂᑕᐱᕆ 52

ᐱᐃ ᒪᓂᐊᓂᑐ, ᕆᖁᖁᕆᐊᕆ ᓂᐅᓂᕮᓂ ᐅ ᖁᑕᑐᑐᓂᖁᕆᕮ ᕆᖁᖁᒪᓂᑐᕮᑫᘐᐅ ᐱᐃ ᓂᖕᑐᐅ ᓂ. ᕆᖁᖁᒪᓂᓀᑐᓂᘓ ᐱᐃ ᒪᓂᐱᐱᓂᐱ ᐅ ᒪᓂᐊᓂᑐ ᘎᓂ ᕮᐅᐅ ᕮᑐᓂ ᐅᘓᕮᐅ ᐅ ᖁᑕᑐᑐᓂᖁᕆ ᐃᐅ ᖁᑕᑐᑐᓂᖁᕆ ᐅ ᐃᐅᐱᕮᐅ ᐅ ᕮᐅᕮᑫᘐᐅ ᓂᖕᑐᐅ ᓂ, ᑐ ᖁᓀᖁᓂᑐᖁ ᖁᓂᖕᑐᑐᓂᖁᓂᖁ ᕮᖁᖁᒪᓂᑕᒣᐅ ᕮ ᖁᓂᐃᐃᓂᐊᖁ ᐅ ᓂᑐᘎᘎᕮᐅ ᕮᖁᖁᒪᓂᘓᕮᓂᐅ, ᓂᑦᓂ ᕮᐃᓂ ᓂᒣᐅᕮᐅ ᐅᐅᕮ ᑐᕮᑕᓂᖁ ᐅᐅᑐ ᐱᓂᖁ ᕮ ᓀᓂ ᒣᐅᕮᐅ ᘎᘎᓂᒣᐅ ᐅ ᓂᑐᘎᘎᕮᐅ ᐅᕮᓀ ᐅᖁᕮᓂᐅᐅᓂ ᐅᐅᑐ.

ᓂᑕᐃᐅᓂᐱ ᒪᕮᑐ ᑐᕮᕮᑐ : ᕮᑐᘓᐱᓂᐱᐅ ᕮᑕᐃᐃᓂᐅᓂ

ᓂᑕᐱᕆ 53

ᕮᖁᖁᓂᐱᒥ ᓂᒣᐅᒥ ᓂ ᐱᐃ ᓂᒣᒣᐃᕮᐅ ᒣᐃ ᓂᑐᓂᘎᓂᐱ ᐅ ᖁᒣᑫᕮᐃᖁ ᐅ ᕮᕮᑫᕮᑐᐅ ᕮᖁᖁᒪᓂᑕᒣᐅ ᕮ ᖁᑐᐅᐅᕮᑐ ᓂᑕᓂᐱᓂᐱ.

ᖁᓄᑭᖁᓂᐊᖅ

ᓄᓇᑐᕼ ᐅᐱᐱᐅᑎ 05.20 ᕿᒪᒪᑎ ᐅ ᖁᑎᑯᐅᓂᖅ ᖁᓄᐅᕿᐊᓕᒐᓂᖅ 6

ᓄᑕᓄᕗᑐᐃᓄ ᓄᑕᖏᒪᓄᑐᐅᐅ : ᕿᐅᐊᕐᓄᐃᓄ ᕿᑕᓄᖁᓄᓴᐃ 6

ᓄᑕᓄᕗᑐᐃᓄ ᒪᐃᕐᐅ ᐅᕿᐃ : ᖁᑕᕗᕗᕿᓴᕿᐃ ᐃ ᐅᕼᑐᓄᕗ ᐃ ᖁᑎᑯᐅᓂᖅ ᐃ ᖁᑎᕗᑐᓄᒪᒪ ᐃ ᒪᐅᑕᑎᓄᐃ 9

ᓄᓴᓴᓄᒪ ᓄᑕᖏᒪᓄᑐᐅ : ᕿᐅᐊᕐᓄᐃᓄ ᕿᖏᑎᕿᐃ ᐅ ᕿᑎᕗᑕᓄᑕᑎ 9

ᓄᓴᓴᓄᒪ ᒪᐃᕐᐅ ᐅᕿᐃ : ᕿᐅᐊᕐᓄᐃᓄ ᕿᖏᑎᕿᐃ ᐅ ᖁᐅᘎᖅᕿᒪᕿᐃ ᖁᕿᓄᐃᐱᐱᓄᒪᕿᐃ ᖁᕿᐱᐅᑎᓄᐃ ᐃ ᒪᐅᑕᑎᓄᐃ ᕿᑕᐅᕼᐅᓄᘎᐃ 11

ᓄᓴᓴᓄᒪ ᒪᐃᕐᐅ ᘎQᓄE: ᕿᐅᐊᕐᓄᐃᓄ ᕿᖏᑎᕿᐃ ᐅ ᕿᑕᓴᓄᒪᒪᓄᑎ 13

ᓄᑕᓄᕗᑐᐃᓄ ᒪᐃᕐᐅ ᘎQᓄE : ᖁᕿᑎᐅᐊEᓄ ᐃ ᖁᑎᑯᐅᓂᖅ ᖁᓄᐅᕿᐊᓕᒐᓂᖅ 15

ᓄᓴᓴᓄᒪ ᓄᑕᖏᒪᓄᑐᐅ : ᖁᓄᐅᒪᒪᕿᑕᖁ ᐃ ᖁᐅᖁᓄᐅᖁᓕᕿᖁ ᐃ ᖁᑎᑯᐅᓂᖅ ᖁᓄᐅᕿᐊᓕᒐᓂᖅ . 15

ᓄᓴᓴᓄᐅ ᒪᐃᕐᐅ ᐅᕿᐃ : ᖁᓄᐃᐊᓄᕿ ᖁᓄᐃᑕᐅᐅᖁ ᐃ ᖁᑎᑯᐅᓂᖅ ᖁᓄᐅᕿᐊᓕᒐᓂᖅ 17

ᓄᑕᓄᕗᑐᐃᓄ ᒪᐃᕐᐅ ᘎᘎᐅᒥ : ᓄᐅᑕᐅᖁᖁᕆ ᐱ ᐅᐅᕼᑐᑎᘎ ᐱ ᐅᑕᓴᓄᒪᓄᐅ 19

ᓄᑕᓄᕗᑐᐃᓄ ᒪᐃᕐᐅ ᐅᑕᑕᐅᐅ : ᓄᐊᐱᐱᕿ ᘎᕼ ᒪᐅᐃᐅᕼᐃ ᐱ ᖁᑕᐅᐅᐅᖁᕿᐃ 20

ᓄᑕᓄᕗᑐᐃᓄ ᒪᐃᕐᐅ ᙃᕮᕿᙃ : ᕿᐅᐊᕐᓄᐃᓄ ᕿᑕᘎᘎᐅᑐᓄ 22

الأمن السيبراني

الأمن السيبراني

2024

ظهير شريف رقم 1.20.69 صادر في 4 ذي الحجة 1441 (25 يوليو 2020)) بتنفيذ القانون رقم 05.20 المتعلق بالأمن السيبراني[1]

الحمد لله وحده،
الطابع الشريف - بداخله :
(محمد بن الحسن بن محمد بن يوسف الله وليه)

يعلم من ظهيرنا الشريف هذا، أسماه الله وأعز أمره أننا:

بناء على الدستور ولا سيما الفصلين 42 و50 منه، أصدرنا أمرنا الشريف بما يلي:

ينفذ وينشر بالجريدة الرسمية، عقب ظهيرنا الشريف هذا، القانون رقم 05.20 المتعلق بالأمن السيبراني، كما وافق عليه مجلس النواب ومجلس المستشارين.

وحرر بتطوان في 4 ذي الحجة 1441 (25 يوليو 2020).

وقعه بالعطف :

رئيس الحكومة،
الإمضاء : سعد الدين العثماني.

1 الجريدة الرسمية عدد 6904 بتاريخ 9 ذو الحجة 1441 (30 يوليو 2020) ؛ ص 4160

قانون رقم 05.20
يتعلق بالأمن السيبراني

الفصل الأول: أحكام عامة

المادة الأولى

يحدد هذا القانون:

- قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام، يشار إليهم في هذا القانون؛
- قواعد ومقتضيات الأمن المطبقة على البنيات التحتية ذات الأهمية الحيوية؛
- قواعد ومقتضيات الأمن المطبقة على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت، يشار إليهم في هذا القانون ب »المتعهد« ؛
- الإطار الوطني لحكامة الأمن السيبراني؛
- إطار التعاون وتبادل المعلومات بين السلطة الوطنية للأمن السيبراني المحددة بنص تنظيمي، والمشار إليها في هذا القانون ب» السلطة الوطنية « والمصالح المختصة للدولة المكلفة بمعالجة الجرائم الماسة بنظم المعالجة الآلية للمعطيات؛
- المساهمات التي تقدمها السلطة الوطنية للهيئات الوطنية المختصة من أجل تعزيز الثقة الرقمية، وتطوير رقمنة الخدمات المقدمة من طرف الدولة، وحماية المعطيات ذات الطابع الشخصي
- اختصاصات السلطة الوطنية لا سيما في ما يتعلق بتطوير الخبرة الوطنية والتحسيس في مجال الأمن السيبراني لفائدة الهيئات والفاعلين في القطاع الخاص والأفراد، وتقوية التعاون مع المؤسسات الوطنية والأجنبية.

المادة 2

يقصد في مدلول هذا القانون بما يلي:

- **الأمـن السـيبراني** :مجموعـة مـن التدابـير والإجـراءات ومفاهيـم الأمـن وطـرق إدارة المخاطـر والأعـمال والتكوينـات وأفضـل الممارسـات والتكنولوجيـات التـي تسـمح لنظـام معلومـات أن يقـاوم أحداثـا مرتبطـة بالفضـاء السـيبراني، مـن شـأنها أن تمـس بتوافـر وسـلامة وسريـة المعطيـات المخزنـة أو المعالجـة أو المرسـلة، والخدمـات ذات الصلـة التـي يقدمهـا هـذا النظـام أو تسـمح بالولـوج إليـه؛

- **جرائـم سـيبرانية** : مجموعـة مـن الأفعـال المخالفـة للتشريـع الوطنـي أو الاتفاقيـات الدوليـة التـي صادقـت عليهـا المملكـة المغربيـة، التـي تسـتهدف شـبكات ونظـم المعلومـات أو تسـتعملها كوسـيلة لارتـكاب جنحـة أو جنايـة؛

- **تهديـد سـيبراني**: كل عمـل يهـدف إلى الإخـلال بأمـن نظـام للمعلومـات مـن خـلال المسـاس بتوافـر النظـام أو المعلومـة التـي يتضمنهـا أو بتماميتهـا أو بسريتهـا؛

- **أخلاقيـات سـيبرانية** : مجموعـة مـن المعايـير والقواعـد التـي تحـدد السـلوك المسـؤول في الفضـاء السـيبراني؛

- **بنيـات تحتيـة ذات أهميـة حيويـة** : التجهيـزات والمنشـآت والأنظمـة الضروريـة للحفـاظ عـلى اسـتمرارية الوظائـف الحيويـة للمجتمـع والصحـة والأمـن والسـلامة والتقـدم الاقتصـادي أو الاجتماعـي حيـث إن أي ضرر أو إتـلاف أو ضيـاع قـد يصيبها يترتـب عنـه خلـل في هـذه الوظائـف

- **قطـاع الأنشـطة ذات الأهميـة الحيويـة** : مجموعـة مـن الأنشـطة التـي تقـوم بهـا البنيـات التحتيـة ذات الأهميـة الحيويـة وتسـاهم في تحقيـق نفـس الهـدف ولهـا علاقـة إمـا بإنتـاج وتوزيـع السـلع أو الخدمـات الضروريـة لتلبيـة الحاجيـات الأساسـية لعيـش المواطنـين، أو بممارسـة الدولـة لصلاحيتهـا أو بالحفاظ عـلى قدراتها الأمنيـة أو بسـير النشـاط الاقتصـادي، عـلى اعتبـار أن هـذه الأنشـطة غـير قابلـة للاسـتبدال أو التعويـض، أو نظـرا للخطـر الجسـيم الـذي قـد تشـكله عـلى السـاكنة؛

- **نظـام معلومـات** : مجموعـة منظمـة مـن المـوارد كالمسـتخدمين والمعـدات والبرامج والمعطيـات والإجـراءات التـي تسـمح بتجميـع المعلومـة في بيئـة معينـة وتصنيفهـا ومعالجتهـا ونشرها؛

- **نظـام معلومـات حسـاس** : نظـام معلومـات يعالـج معلومـات أو معطيات حساسـة مـن شـأن المسـاس بسريتهـا أو بسـلامة محتواهـا أو بتوافرهـا أن يلحـق ضررا بهيئـة مـا أو ببنيـة تحتيـة ذات أهميـة حيويـة؛
- **خدمـة للأمـن السـيبراني** : كل خدمـة أمـن مقدمـة مـن لـدن مقدمـي خدمـات الأمـن السـيبراني لفائـدة هيئـة مـا أو بنيـة تحتيـة ذات أهميـة حيويـة تهـم رصـد وتشـخيص حـادث أمـن سـيبراني وتقويـة أمـن نظـم معلوماتهـا
- مقـدم خدمـات رقميـة »:كل شـخص ذاتي أو اعتبـاري يقـدم عـن بعـد وبطريقـة إلكترونيـة، وبنـاء عـلى طلـب مسـتفيد مـا، إحـدى الخدمـات التاليـة:
- خدمـة رقميـة تسـمح لمسـتهلكين أو لمهنيـين بإبـرام عقـود بيـع أو خدمـة عـبر الإنترنـت؛
- خدمة رقمية تسمح للمستعملين القيام بأبحاث على مواقع الإنترنت؛
- خدمـة رقميـة تسـمح بالولـوج إلى مجموعـة مرنـة ومتنوعة مـن المـوارد المعلوماتية التـي يمكـن تقاسـمها، بمـا فيهـا مسـتضيفي المعطيـات أو نظـم المعلومـات أو هـما معـا ومقدمـي الخدمـات الرقمية السـحابية؛
- إيـواء : كل خدمـة لتخزيـن إشـارات أو كتابـات أو صـور أو أصـوات أو رسـائل بمختلـف أنواعهـا، مقدمـة بعـوض أو بـدون عـوض مـن لـدن مقدمـي الخدمـات الرقميـة؛
- **إسـناد نظـام المعلومـات لجهـة خارجيـة** : كل عمليـة تتمثـل في الإسـناد الجـزئي أو الـكلي لنظـام معلومـات هيئـة مـا إلى مقـدم خدمـات معـين في إطـار عقـد يحـدد بدقـة عـلى الخصـوص مسـتوى الخدمـات ومـدة الإسـناد؛
- **المصادقـة عـلى نظـم المعلومـات** : وثيقـة يشـهد بواسـطتها المسـؤول عـن البنيـة التحتيـة ذات الأهميـة الحيويـة عـلى اطلاعـه عـلى نظـام المعلومـات والتدابـير الأمنيـة التقنيـة أو التنظيميـة أو القانونيـة المتخـذة وعـلى تحملـه للمخاطـر المتبقيـة؛
- **حـادث أمـن سـيبراني** : واقعـة أو وقائـع غـير مرغـوب فيها أو غـير متوقعـة، مرتبطة بأمـن نظـم المعلومـات، والتـي يحتمـل جـدا أن تعـرض للخطـر أنشـطة هيئـة مـا أو بنيـة تحتيـة ذات أهميـة حيويـة أو متعهـد أو أن تهـدد سـلامة نظمهـم المعلوماتية

- **أزمة أمن سيبراني** : حالة ناتجة عن وقوع حدث أو عدة أحداث متعلقة بالأمن السيبراني، يمكن أن يكون لها وقع خطير على حياة الأفراد أو على ممارسة الدولة لسلطاتها أو سير الاقتصاد أو على المحافظة على القدرات الأمنية والدفاعية للبلاد؛
- **إدارة حوادث الأمن السيبراني** : عمليات رصد حوادث الأمن السيبراني والتبليغ عنها وتقييمها وكذا التدابير المتخذة للتدخل والمعالجة المتعلقة بها.

الفصل الثاني : إجراءات حماية أمن نظم المعلومات

الفرع الأول: أحكام خاص بالهيئات

المادة 3

يجب على كل هيئة أن تسهر على أن تكون نظم معلوماتها مطابقة للتوجيهات والقواعد والأنظمة والمراجع والتوصيات الصادرة عن السلطة الوطنية.

المادة 4

يجب على كل هيئة أن تضع وتنفذ سياسة لأمن نظم معلوماتها وفق التوجيهات الصادرة عن السلطة الوطنية. يجب على كل هيئة تحديد المخاطر التي تهدد أمن نظم معلوماتها واتخاذ الإجراءات التقنية والتنظيمية اللازمة لإدارة هذه المخاطر، من أجل تجنب الحوادث التي من شأنها المساس بنظم المعلومات وكذا التقليل إلى أدنى حد ممكن من الآثار التي قد تنجم عن هذه الحوادث. يجب أن يخضع كل نظام معلومات هيئة تقدم خدمات رقمية للغير لا فتحاص أمني قبل الشروع في استغلاله. يجب على كل هيئة إجراء افتحاص لنظم معلوماتها بانتظام.

المادة 5

يجب على كل هيئة أن تقوم بتصنيف أصولها المعلوماتية ونظم معلوماتها حسب مستوى حساسيتها من حيث السرية والتمامية والتوافر، كما يتعين أن تكون تدابير حماية الأصول المعلوماتية ونظم المعلومات متناسبة مع مستوى التصنيف المخصص لها. يجب على كل هيئة أن تحدد إجراءات تأهيل الأشخاص الذين يمكنهم الولوج إلى المعلومات المصنفة وشروط معالجة هذه المعلومات أو

تبادلها أو تخزينها أو نقلها. يحدد بنص تنظيمي الدليل المرجعي لتصنيف أصول المعلومات ونظم المعلومات.

المادة 6

يجب على كل هيئة أن تعين مسؤولا عن أمن نظم المعلومات، يتولى السهر على تطبيق سياسة أمن نظم المعلومات. يعتبر المسؤول عن أمن نظم المعلومات مخاطب السلطة الوطنية للأمن السيبراني، ويتعين أن يتمتع بالاستقلالية اللازمة لممارسة مهامه.

المادة 7

يجب على كل هيئة أن توفر الوسائل المناسبة لمراقبة ورصد الأحداث التي قد تمس بأمن نظم معلوماتها ويكون لها وقع بالغ على استمرارية الخدمات التي تقدمها. لا يمكن للسلطة الوطنية استغلال المعطيات التقنية المحصل عليها بواسطة الوسائل المذكورة إلا لغرض تحديد ومعالجة الخطر الذي يمس بأمن نظم معلومات الهيئة المعنية.

المادة 8

يجب على كل هيئة فور علمها بأي حادث يؤثر على أمن أو سير نظم المعلومات الخاصة بها أن تقوم بإبلاغ السلطة الوطنية. تقوم كل هيئة بإبلاغ السلطة الوطنية، بناء على طلب هذه الأخيرة، ودون تأخير، بالمعلومات الإضافية المتعلقة بالحوادث التي تؤثر على أمن أو سير نظم معلوماتها. تبين السلطة الوطنية المعطيات التقنية والمعلومات المتعلقة بالحوادث، التي يجب إبلاغها، وكذا كيفيات إرسالها ترسل السلطة الوطنية إلى الهيئة المعنية تقريرا تركيبيا يتضمن التدابير والتوصيات لمعالجة الحادث.

المادة 9

تعد كل هيئة مخططا لضمان استمرارية أو استئناف الأنشطة يتضمن مجموع الحلول البديلة لإبطال مفعول انقطاعات الأنشطة وحماية الوظائف المهمة والحساسة من الآثار الناجمة عن الاختلالات الأساسية لنظم المعلومات أو عن الكوارث، وضمان استئناف عمل هذه الوظائف في أقرب الآجال. يتعين اختبار مخطط ضمان استمرارية أو استئناف الأنشطة بصفة منتظمة من أجل تحيينه حسب التطورات الخاصة بالهيئة وتطور التهديدات.

المادة 10

في حالة إسناد نظام معلومات حساس لجهة خارجية، يجب على هذه الجهة احترام القواعد والأنظمة والدلائل المرجعية التقنية المتعلقة بأمن نظم المعلومات، والتي تضعها السلطة الوطنية.

المادة 11

يجب أن يتم إيواء المعطيات الحساسة، حصريا، داخل التراب الوطني.

المادة 12

يجب أن يكون كل إسناد خارجي لنظام معلومات حساس موضوع عقد خاضع للقانون المغربي، يتضمن وجوبا الالتزامات المتعلقة بحماية المعلومة وقابليتها للافتحاص واستعادتها، وكذا متطلبات الأمن ومستوى الخدمة المرغوب فيها.

المادة 13

تحدد السلطة الوطنية القواعد والدليل المرجعي التقني المنظم لشروط الأمن المتعلقة بالإسناد الخارجي لنظم المعلومات.

الفرع الثاني : أحكام خاصة بالبنيات التحتية ذ ات الأهم المتوفرة على نظم معلومات حساسة

المادة 14

تسري أحكام الفرع الأول من هذا الفصل على البنيات التحتية ذات الأهمية الحيوية.

المادة 15

تحدد بنص تنظيمي لائحة قطاعات الأنشطة ذات الأهمية الحيوية وكذا السلطات الحكومية والمؤسسات العمومية وباقي الأشخاص الاعتباريين الخاضعين للقانون العام المشرفين على تنسيق هذه القطاعات.

المادة 16

يتـم تحديـد البنيـات التحتيـة ذات الأهميـة الحيويـة لـكل قطـاع أنشـطة ذات أهميـة حيويـة، بعـد اسـتطلاع رأي السـلطة الوطنيـة، مـن طـرف السـلطة الحكوميـة أو المؤسسـة العموميـة أو الشـخص الاعتبـاري الخاضـع للقانـون العـام المـشرف عـلى تنسـيق هـذا القطـاع تظـل لائحـة هـذه البنيـات التحتيـة سريـة، ويتـم تحيينهـا عـلى فـترات منتظمـة لا تتعـدى سـنتين.

المادة 17

يقـوم المسـؤول عـن البنيـة التحتيـة ذات الأهميـة الحيويـة، بنـاء عـلى نتائـج تحليـل المخاطـر، بإعـداد لائحـة نظـم المعلومـات الحساسـة، وإرسـالها في صيغتهـا المحينـة إلى السـلطة الوطنيـة.

المادة 18

يمكـن للسـلطة الوطنيـة توجيـه ملاحظـات إلى المسـؤول عـن البنيـة التحتيـة ذات الأهميـة الحيويـة بخصـوص لائحـة نظـم المعلومـات الحساسـة التـي تمـت موافاتهـا بهـا. في هـذه الحالـة، يتعـين عـلى المسـؤول عـن البنيـة التحتيـة ذات الأهميـة الحيوية تعديـل لائحتهـا وفقـا لهـذه الملاحظـات، وإرسـال اللائحة المعدلـة إلى السـلطة الوطنية داخـل أجـل شـهرين مـن تاريـخ التوصـل بالملاحظـات. تظـل لائحـة نظـم المعلومـات الحساسـة سريـة.

المادة 19

يجـب أن يخضـع أمـن كل نظـام معلومـات حسـاس للمصادقـة قبـل الـشروع في اسـتغلاله. تحـدد السـلطة الوطنيـة دليـل المصادقـة عـلى نظـم المعلومـات الحساسـة.

المادة 20

يجـب عـلى المسـؤولين عـن البنيـات التحتيـة ذات الأهميـة الحيويـة، بنـاء عـلى طلـب مـن السـلطة الوطنيـة، إخضـاع نظـم المعلومـات الحساسـة الخاصـة بهـا إلى افتحـاص تقـوم بـه هـذه السـلطة أو متعهـدي الافتحـاص المؤهلـين مـن قبلهـا. تحـدد بنـص تنظيمـي معايـير تأهيـل متعهـدي الافتحـاص وكـذا كيفيـات إجـراء الافتحـاص.

المادة 21

يجب على المسؤولين عن البنيات التحتية ذات الأهمية الحيوية مد السلطة الوطنية أو متعهد الافتحاص المؤهل بالمعلومات والعناصر اللازمة لإجراء الافتحاص، بما في ذلك الوثائق المتعلقة بسياستها الأمنية، وعند الاقتضاء، نتائج الافتحاص الأمني السابقة، والسماح لهم بالولوج إلى الشبكات ونظم المعلومات موضوع المراقبة قصد إجراء التحليلات واستخراج بيانات المعلومات التقنية.

يجب أن يلتزم متعهدو الافتحاص المؤهلون ومستخدموهم، تحت طائلة العقوبات المنصوص عليها في مجموعة القانون الجنائي، باحترام السر المهني طيلة مدة مهمة الافتحاص وبعد الانتهاء منها، بشأن المعلومات والوثائق التي تم تجميعها أو اطلعوا عليها أثناء القيام بهذه المهمة.

المادة 22

في حالة إجراء الافتحاص من طرف متعهد افتحاص مؤهل، يقوم المسؤول عن البنية التحتية ذات الأهمية الحيوية بإرسال تقرير الافتحاص إلى السلطة الوطنية يجب على متعهد الافتحاص المؤهل أن يسهر على ضمان سرية تقرير الافتحاص.

المادة 23

عند إجراء عمليات الافتحاص من طرف متعهدي الافتحاص المؤهلين، يتحمل المسؤول عن البنية التحتية ذات الأهمية الحيوية المعنية مصاريف هذه العمليات.

المادة 24

يجب على كل مسؤول عن بنية تحتية ذات أهمية حيوية تم افتحاصها وضع برنامج عمل لتنفيذ التوصيات الواردة في تقارير الافتحاص، وإرساله إلى السلطة الوطنية قصد تتبع تنفيذه.

المادة 25

يجب أن يلجأ المسؤولون عن البنيات التحتية ذات الأهمية الحيوية إلى الخدمات أو المنتوجات أو الحلول التي تسمح بتعزيز الوظائف الأمنية، والتي تحددها السلطة الوطنية. في حالة إسناد خدمات الأمن السيبراني لجهة خارجية، يجب على المسؤولين عن البنيات التحتية ذات الأهمية الحيوية اللجوء إلى مقدمي

خدمات مؤهلين من طرف السلطة الوطنية. تحدد بنص تنظيمي معايير تأهيل مقدمي خدمات الأمن السيبراني.

الفرع الثالث: أحكام خاص بالمتعهدين

المادة 26

يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت التقيد بتوجيهات السلطة الوطنية، لا سيما تلك المتعلقة بالمحافظة على المعطيات التقنية اللازمة لتحديد أي حادث أمن سيبراني. تتضمن هذه المعطيات التقنية على الخصوص، بيانات الربط والنشرات المعلوماتية وآثار أحداث الأمن المحصل عليها بواسطة نظم الاستغلال والتطبيقات ومنتوجات الأمن. تحدد مدة الاحتفاظ بالمعطيات التقنية اللازمة لتحديد وتحليل الحادث في سنة واحدة، ويمكن تغيير هذه المدة بنص تنظيمي.

المادة 27

يخطر مستغلو الشبكات العامة للمواصلات ومزودو خدمات الإنترنت ومقدمو خدمات الأمن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الإنترنت بناءهم بهشاشة نظم معلوماتهم أو الانتهاك الذي قد يطالها.

المادة 28

من أجل ضمان أمن نظم المعلومات الخاصة بالهيئات والبنيات التحتية ذات الأهمية الحيوية، يسمح لأعوان السلطة الوطنية المعتمدين حصريا بهدف الوقاية وتحديد خصائص التهديد السيبراني، بتجميع وتحليل المعطيات التقنية، دون أي استغلال آخر، لدى مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت تؤهل السلطة الوطنية لوضع أجهزة تقنية على الشبكات العامة للمواصلات وشبكات مزودي خدمات الإنترنت حصريا بهدف رصد الأحداث التي قد تؤثر على أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية. توضع هذه الأجهزة حصريا خلال المدة وفي الحدود التي يتطلبها تحديد خصائص التهديد.

المادة 29

يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت، في إطار توجيهات السلطة الوطنية، اتخاذ التدابير الحمائية اللازمة لأجل الوقاية وإبطال مفعول التهديدات أو الانتهاكات التي تمس نظم معلومات زبنائهم.

المادة 30

عندما يقوم مستغلو الشبكات العامة للمواصلات ومزودو خدمات الإنترنت ومقدمو خدمات الأمن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الإنترنت برصد أحداث قد تؤثر على أمن نظم بذلك. معلومات زبنائهم، وجب عليهم إخطار السلطة الوطنية فورا

المادة 31

يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت أن يستعملوا، في شبكات الاتصالات الإلكترونية التي يستغلونها، أجهزة للرصد تشتغل بعلامات تقنية توفرها السلطة الوطنية، وذلك فقط بهدف رصد الأحداث التي قد تؤثر على أمن نظم معلومات مشتركيها.

المادة 32

يجب على مقدمي الخدمات الرقمية تحديد المخاطر التي تهدد أمن نظم معلوماتهم، واتخاذ التدابير التقنية والتنظيمية اللازمة لإدارة هذه المخاطر، وذلك لمنع وقوع الحوادث التي قد تؤثر سلبا على هذه الشبكات ونظم المعلومات، والتقليل إلى أدنى حد ممكن من أثر هذه المخاطر ضمانا لاستمرارية هذه الخدمات.

المادة 33

يجب على مقدمي الخدمات الرقمية، فور علمهم بأي حوادث تؤثر على الشبكات ونظم المعلومات اللازمة لتوفير خدماتهم، أن يقوموا بإبلاغ السلطة الوطنية بها، وذلك حينما يتبين من المعلومات المتوفرة لديهم أن لهذه الحوادث وقع بالغ يؤثر على تقديم هذه الخدمات.

المادة 34

إذا تـم، بـأي وسـيلة كانـت، إخبـار السـلطة الوطنيـة بـأن أحـد مقدمـي الخدمـات الرقميـة لا يفـي بأحـد الالتزامـات المنصـوص عليهـا في هـذا القانـون، أمكـن لهـذه السـلطة أن تخضعـه للمراقبـة مـن أجـل التحقـق مـن تقيـده بهـذه الالتزامـات، وكـذا مـن مسـتوى أمـن الشـبكات ونظـم المعلومـات اللازمـة لتقديم خدماتـه. تتـم المراقبة مـن قبـل السـلطة الوطنيـة أو مـن قبـل متعهـدي الافتحـاص المؤهلـين مـن قبـل هذه السـلطة .وفي هـذه الحالـة الأخـيرة، يتحمـل مقـدم الخدمـات الرقميـة مصاريـف عمليـات المراقبـة. إذا تبـين أثنـاء إجـراء المراقبـة وجـود أي إخـلال بالالتزامـات الملقـاة عـلى عاتـق مقـدم الخدمـات بموجـب هـذا الفـرع، أمكـن للسـلطة الوطنيـة إعـذار مسـيري مقـدم الخدمـات المعنـي بالتقيـد بهـذه الالتزامـات، وذلـك داخـل أجـل تحـدده هـذه السـلطة.

الفصل الثالث: حكامة الأمن السيبراني

الفرع الأول: اللجنة الاستراتيجية للأمن السيبراني

المادة 35

تحدث لجنة استراتيجية للأمن السيبراني، يعهد إليها بالقيام بما يلي:

- إعـداد التوجهـات الاسـتراتيجية للدولـة في مجـال الأمـن السـيبراني والسـهر عـلى ضـمان صمـود نظـم معلومـات الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة والمتعهديـن المشـار إليهـم في الفـرع الثالـث مـن الفصـل الثـاني مـن هـذا القانـون؛
- التقييم السنوي لأنشطة السلطة الوطنية؛
- تقييـم عمـل اللجنـة الوطنيـة لإدارة الأزمـات والأحـداث السـيبرانية الجسـيمة، المنصـوص عليهـا في المـادة 36 بعـده؛
- حصر نطاق افتحاصات أمن نظم المعلومات التي تنجزها السلطة الوطنية؛
- تشجيع البحث والتطوير في مجال الأمن السيبراني؛
- تشـجيع برامـج وأنشـطة التحسـيس وتعزيـز القـدرات في مجـال الأمـن السـيبراني لفائـدة الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة؛

- إبـداء الـرأي في مشـاريع القوانـين والنصـوص التنظيميـة المتعلقـة بمجـال الأمـن السـيبراني.

يحدد بنص تنظيمي تأليف وكيفيات سير اللجنة الاستراتيجية للأمن السيبراني.

المادة 36

تحـدث لـدى اللجنـة الاسـتراتيجية للأمـن السـيبراني، لجنـة لإدارة الأزمـات والأحـداث السـيبرانية الجسـيمة، تكلـف بضـمان تدخـل منسـق في مجـال الوقاية وتدبـير الأزمات عـلى إثـر وقـوع حـوادث أمـن سـيبراني. ولهـذا الغـرض، يتعين على مسـتغلي الشـبكات العامـة للمواصـلات ومـزودي خدمـات الإنترنـت ومقدمـي خدمـات الأمـن السـيبراني ومقدمـي الخدمـات الرقميـة الامتثـال للأوامـر الصـادرة عـن لجنـة إدارة الأزمـات والأحـداث السـيبرانية الجسـيمة والاسـتجابة لطلباتهـا المتعلقـة بالدعـم والمسـاعدة التقنيـة. يحـدد بنـص تنظيمـي تأليـف اللجنـة وكيفيـات اشـتغالها ومجـال تدخـل كل عضـو مـن أعضائهـا.

المادة 37

يمكـن للجنـة إدارة الأزمـات والأحـداث السـيبرانية الجسـيمة، مـن أجـل التصـدي لحـوادث الأمـن السـيبراني الجسـيمة، أن تحـدد التدابـير التـي يتوجـب عـلى مسـؤولي الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة تنفيذهـا وأن تقـدم توصيـات ونصائـح إلى متعهـدي القطـاع الخـاص والأفـراد.

الفرع الثاني: السلطة الوطنية للأمن السيبراني

المادة 38

يعهـد إلى السـلطة الوطنيـة بتنفيـذ اسـتراتيجية الدولـة في مجـال الأمـن السـيبراني. ولهـذا الغـرض، تتـولى السـلطة الوطنيـة، عـلاوة عـلى المهـام الأخـرى المسـندة إليهـا بمقتـضى هـذا القانـون، القيـام بالمهـام التاليـة :

- تنسـيق الأعـمال المتعلقـة بإعـداد وتنفيـذ اسـتراتيجية الدولـة في مجـال الأمـن السـيبراني والسـهر عـلى ضـمان تطبيـق توجيهـات اللجنـة الاسـتراتيجية للأمـن السـيبراني؛
- تحديد تدابير حماية نظم المعلومات والسهر على ضمان تطبيقها؛

- تقديم اقتراحات إلى اللجنة الاستراتيجية للأمن السيبراني بخصوص تدابير التصدي للأزمات التي تمس أو تهدد أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية؛
- تأهيل مقدمي خدمات افتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية ومقدمي خدمات الأمن السيبراني؛
- وضع تصور للوسائل اللازمة لضمان أمن الاتصالات الإلكترونية بين الوزارية وتنسيق تفعيلها؛
- القيام بأعمال المراقبة المنصوص عليها في هذا القانون؛
- السهر على ضمان إجراء عمليات افتحاص أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية؛
- افتحاص متعهدي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الذين يقدمون خدمات للبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة
- تقديم المساعدة والنصائح إلى الهيئات والبنيات التحتية ذات الأهمية الحيوية قصد تعزيز أمن نظم معلوماتها؛
- مساعدة ومواكبة الهيئات والبنيات التحتية ذات الأهمية الحيوية لوضع أجهزة لرصد أحداث مست أو قد تمس بأمن نظم معلوماتها وكذا تنسيق إجراءات التصدي لهذه الأحداث؛
- القيام، بتعاون مع الهيئات والبنيات التحتية ذات الأهمية الحيوية، بإعداد نظام خارجي لليقظة والرصد والإنذار بأحداث مست أو قد تمس بأمن نظم معلوماتها وكذا تنسيق إجراءات التصدي لهذه الأحداث؛
- القيام بأنشطة البحث العلمي والتقني في مجال الأمن السيبراني وتشجيعها.

المادة 39

يتعين على السلطة الوطنية ضمان سرية المعلومات الحساسة التي تجمعها في إطار هذا القانون.

المادة 40

تحـدد السـلطة الوطنيـة قواعـد الأمـن اللازمـة لحمايـة نظـم معلومـات الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة والمتعهديـن المشـار إليهـم في المـادة الأولى مـن هـذا القانـون.

تحـدد السـلطة الوطنيـة قواعـد أمـن خاصـة بقطـاع أنشـطة ذي أهميـة حيويـة معـين. وتقـوم بتبليـغ هـذه القواعـد وكـذا كيفيـات وآجـال تطبيقهـا إلى مسـؤولي البنيـات التحتيـة ذات الأهميـة الحيويـة التابعـين للقطـاع المعنـي. يجـب عـلى المسـؤولين سـالفي الذكـر تطبيـق هـذه القواعـد عـلى نفقتهـم.

المادة 41

لأجـل التصـدي لأي هجـوم إلكـتروني يسـتهدف نظـم المعلومـات ويمـس بالوظائـف الحيويـة للمجتمـع أو الصحـة أو السـلامة أو الأمـن أو التقـدم الاقتصـادي أو الاجتماعـي، يقـوم أعـوان السـلطة الوطنيـة بالتحريـات التقنيـة اللازمـة لتحديـد خصائـص الهجـوم ويسـهرون عـلى ضـمان تنفيـذ التدابـير والتوصيـات المتعلقـة بهـا.

المادة 42

تتعـاون السـلطة الوطنيـة مـع المصالـح المختصـة في الدولـة مـن خـلال تبـادل أي معطيـات أو معلومـات قـد تسـاعدها عـلى معالجـة الجرائـم التـي تخـل بسـير نظـم المعالجـة الآليـة للمعطيـات.

إذا تبـين للسـلطة الوطنيـة، أثنـاء ممارسـة مهامهـا، وجـود فعـل يشـتبه في مخالفتـه للقانـون، فإنهـا تحيـل الأمـر إلى السـلطات المختصـة. يتعـين عـلى السـلطات المختصـة إخبـار السـلطة الوطنيـة بالمـآل المخصـص للإحالـة

الفصل الرابع : التكوين والتحسيس والتعاون

المادة 43

تقـوم السـلطة الوطنيـة، بتعـاون مـع الفاعلـين والمهنيـين في مجـال الأمـن السـيبراني، بتنظيـم دورات تكوينيـة وتمارِيـن لفائـدة مسـتخدمي الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة مـن أجـل تطويـر وتعزيـز القـدرات الوطنيـة في هـذا المجـال.

المادة 44

تقـوم السـلطة الوطنيـة بتحديـد وتنفيـذ برامـج تحسيسـية بشـأن الأخلاقيـات السـيبرانية والتحديـات المتعلقـة بتهديـدات ومخاطـر الأمـن السـيبراني لفائـدة مسـتخدمي الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة والقطـاع الخـاص والأفـراد. تنـشر بانتظـام عـلى الموقـع الإلكتروني للسـلطة الوطنيـة النصائـح والتوصيات الوقائيـة المتعلقـة بالأمـن السـيبراني لفائـدة مسـتخدمي الهيئـات والبنيـات التحتيـة ذات الأهميـة الحيويـة والقطـاع الخـاص والأفـراد.

المادة 45

تسـهم السـلطة الوطنيـة في دعـم البرامـج التـي تعدهـا الهيئـات المختصـة في الدولـة مـن أجـل تعزيـز الثقـة الرقميـة وتطويـر رقمنـة الخدمـات وحمايـة المعطيـات ذات الطابـع الشـخصي.

المادة 46

تقـوم السـلطة الوطنيـة، بتشـاور مـع الإدارات المعنيـة، بتطويـر علاقـات التعـاون مـع المنظـمات الوطنيـة والأجنبيـة في مجـال الأمـن السـيبراني وتنسـيقها.

المادة 47

تقـوم السـلطة الوطنيـة بربـط علاقـات التعـاون عـلى الصعيديـن الوطنـي والـدولي لمعالجـة حـوادث الأمـن السـيبراني وتطويـر تبـادل التجـارب والخـبرات في هـذا المجال.

الفصل الخامس : معاينة المخالفات والعقوبات

المادة 48

يؤهـل للبحـث عـن المخالفـات لأحـكام هـذا القانـون والنصـوص المتخـذة لتطبيقـه ومعاينتهـا بواسـطة محـاضر، عـلاوة عـلى ضبـاط الشرطـة القضائيـة، أعـوان السـلطة الوطنيـة المنتدبـون لهـذا الغـرض والمحلفـون وفـق التشريـع الجـاري بـه العمـل توجه محـاضر معاينـة المخالفـات إلى النيابـة العامـة المختصـة.

المادة 49

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 200.000 إلى 400.000 درهم -كل مسؤول عن هيئة أو بنية تحتية ذات أهمية حيوية قام بإيواء:

- كل مسؤول عن بنية تحتية ذات أهمية حيوية تتوفر على نظام المعطيات الحساسة خارج التراب الوطني، خرقا لأحكام المادة 11 أعلاه؛
- معلومات حساس شرع في استغلاله دون إخضاعه للمصادقة المنصوص عليها في المادة 19 أعلاه؛
- كل مسؤول عن بنية تحتية ذات أهمية حيوية عهد بافتحاص أمن نظم المعلومات الحساسة الخاصة ببنيته التحتية إلى متعهد افتحاص غير مؤهل، خرقا لأحكام المادة 20 أعلاه؛
- كل من قدم خدمات افتحاص أمن نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية دون أن يكون مؤهلا من قبل السلطة الوطنية أو استمر في تقديم هذه الخدمات رغم سحب تأهيله من قبل هذه السلطة؛
- كل مسؤول عن بنية تحتية ذات أهمية حيوية أسند خدمات الأمن السيبراني إلى مقدم خدمات غير مؤهل، خرقا لأحكام المادة 25 أعلاه؛
- كل من قدم خدمات الأمن السيبراني دون أن يكون مؤهلا من قبل السلطة الوطنية أو استمر في تقديم هذه الخدمات رغم سحب تأهيله من قبل هذه السلطة.

المادة 50

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 100.000 إلى 200.000 درهم:

- كل من أخل بالالتزامات المتعلقة بإبلاغ السلطة الوطنية عن الحوادث، خرقا لأحكام المواد 8 و 30و 33أعلاه؛
- كل من قام، بأي وسيلة كانت، بعرقلة أو بمنع إجراء عمليات افتحاص أمن نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، المنصوص عليها في المادة 20 أعلاه؛

- كل متعهد لشبكة عامة للمواصلات أو مزود خدمات الإنترنت أو مقدم خدمات الأمن السيبراني أو مقدم الخدمات الرقمية أو ناشر منصات الإنترنت أخل بالالتزامات المنصوص عليها في المادة 26 أعلاه؛
- كل متعهد لشبكة عامة للمواصلات أو مزود خدمات الإنترنت أو أعوانهم، عرقل أعمال السلطة الوطنية أو أعوانها المنصوص عليها في المادة 28 أعلاه؛
- كل مقدم خدمة رقمية امتنع عن اتخاذ التدابير المنصوص عليها في المادة 32 أعلاه أو عرقل عمليات المراقبة المنصوص عليها في المادة 34 أعلاه يعاقب بالغرامة نفسها كل شخص اسْتُخْدِم نظام معلوماته دون علمه لنشر البرمجيات الخبيثة أو للقيام بأعمال مخالفة للقانون، امتنع عن تنفيذ توجيهات السلطة الوطنية بعد إخباره بها.

المادة 51

يجوز للمحكمة أن تحكم بمصادرة المواد والوسائل التي استعملت لارتكاب أفعال مخالفة لأحكام هذا القانون.

المادة 52

في حالة العود، ترفع العقوبات المنصوص عليها في هذا القانون إلى الضعف. يعتبر في حالة العود كل من سبق الحكم عليه بعقوبة من أجل ارتكاب إحدى المخالفات المنصوص عليها في هذا القانون بمقرر قضائي مكتسب لقوة الشيء المقضي به، ثم ارتكب نفس المخالفة قبل مضي أربع سنوات من تمام تنفيذ تلك العقوبة أو تقادمها.

الفصل السادس : أحكام ختامية

المادة 53

يدخل هذا القانون حيز التنفيذ ابتداء من تاريخ نشر النصوص المتخذة لتطبيقه بالجريدة الرسمية.

فهرس

قانون رقم 05.20 يتعلق بالأمن السيبراني 5

الفصل الأول : أحكام عامة 6

الفصل الثاني : إجراءات حماية أمن نظم المعلومات 9

الفرع الأول : أحكام خاص بالهيئات 9

الفرع الثاني : أحكام خاصة بالبنيات التحتية ذ ات الأهم المتوفرة على نظم معلومات حساسة 11

الفرع الثالث : أحكام خاص بالمتعهدين 14

الفصل الثالث : حكامة الأمن السيبراني 16

الفرع الأول : اللجنة الاستراتيجية للأمن السيبراني 16

الفرع الثاني : السلطة الوطنية للأمن السيبراني 17

الفصل الرابع : التكوين والتحسيس والتعاون 19

الفصل الخامس : معاينة المخالفات والعقوبات 20

الفصل السادس : أحكام ختامية 22

فهرس 23

ⵖⵓⴰⵅ ⵍⵛⵢⵙⵜⵜ ⴰⵄ ⵜⵣⵔⵣⵜ ⵏ ⵓⵙⵜⵓⵢⵍⵓⵙ ⵏ ⵜⵣⵛⵛⵙⵙ ⵜⵉⵏⵛⵓⵙⵜⵉ ⵏ ⵜⵏⵅⵙⵓⵜ ⵏ ⵉⵏⵔⵙⵙⵓⵍⵏ ⵏ ⵓⵓⵛⵍⵏⵙ ⴰ ⵓⵙⴰⵓⵙ ⵏ ⵜⵛⵖⵛⵛⵙⵏⵜ ⵜⵙⵛⵓⵓⵜⵜⵓⵜ. ⵜⵙⵙⵓⵏⴰ ⵜⵛⵙⵙⵓⵓⵙⵙ ⵏ ⵓⵛⵣⵙⵙ ⵙⵏⵙⵙⵓ 05.20 ⵉⵓⵓⵏ ⵙ ⵜⵏⵅⵙⵓⵜ ⵜⵙⵙⵜⵜⵙⵙⵏⵉⵜ, ⵉⵓⵙⵜⵙⵏ ⵙⵙⴰⵓⵙ ⵏ ⵓⵅⵙⵙⵙ ⴰ ⵓⵙⴰⴰⵉ ⵏ ⵉⵏⵔⵙⵙⵓⵍⵏ ⴰ ⵓⵛⵏⵙⵏⵙ ⵏ ⵜⵓⵔⵉⵙ ⵜⵙⵙⵜⵜⵙⵙⵏⵉⵜ, ⴰ ⵓⵙⴰⵓⵙ ⵏ ⵜⵙⵛⵓⵓⵜⵜⵓⵜ, ⴰ ⵓⵅⵙⵙⵙ ⵏ ⵓⵓⵛⵍⵏⵙ ⵉⵏⵉⵛⵙⵏⵏ ⴰ ⵉⵛⵏⵜⵙⵏⵏ, ⴰ ⵜⵉⵔⵔⵉ ⵉ ⵜⵙⵙⵔⵔⵉⵛⵜ ⵜⵙⵙⵜⵙⵙⵜⵉⵉⵜ ⴰ ⵜⵏⵙⵙⵉⵜ ⵜⵙⵙⵓⵛⵍⵏⵙⵙⵜ ⵏ ⵓⵓⵛⵍⵏⵙ, ⴰ ⵓⵙⴰⵓⵙ ⴰ ⵓⵙⵙⵙⵜⵜⵙⵙⵏⵉⵜ ⵏ ⵜⵓⵍⵍⵙⵉⵜ ⵜⵙⵙⵓⵛⵍⵏⵙⵙⵜ ⵏ ⵜⵏⵅⵙⵓⵜ ⵜⵙⵙⵜⵜⵙⵙⵏⵉⵜ.

* * * * *

انخرط المغرب في مسار تطوير القدرات الوطنية لأمن نظم المعلومات وتعزيز الثقة الرقمية. حيث قامت إدارة الدفاع الوطني بإعداد القانون رقم 05.20 المتعلق بالأمن السيبراني، والذي يهدف إلى تعزيز حماية وصمود نظم المعلومات ومواجهة الهجمات السيبرانية، وتعزيز الرقمنة، وحماية المعطيات الشخصية والحساسة، وتخويل اللجنة الاستراتيجية والسلطة الوطنية صلاحيات ووسائل الاضطلاع بمهمة حماية نظم المعلومات، وتعزيز وتطوير البيئة الوطنية للأمن السيبراني.